

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning documents *will not* correct images,  
Please do not report the images to the  
Image Problem Mailbox.

#2

**THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re the Application of : Yoichiro IGARASHI, et al.

Filed : Concurrently herewith

For : MOBILE COMMUNICATIONS SYSTEM...

Serial No. : Concurrently herewith

February 5, 2001

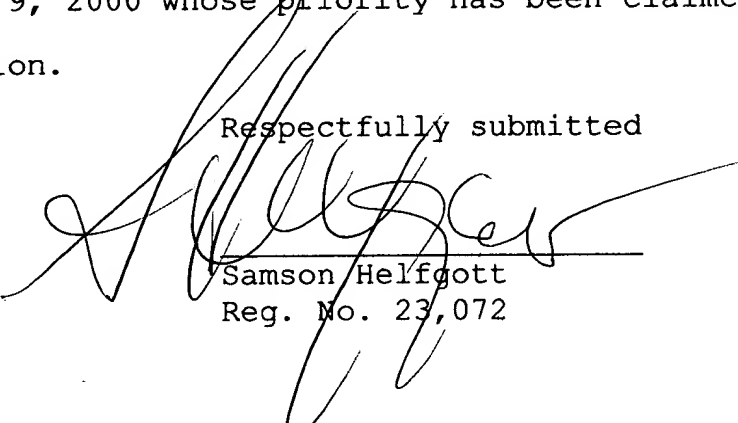
Assistant Commissioner of Patents  
Washington, D.C. 20231

**SUBMISSION OF PRIORITY DOCUMENT**

S I R:

Attached herewith are Japanese patent application No.  
2000-032372 of February 9, 2000 whose priority has been claimed  
in the present application.

Respectfully submitted

  
Samson Helfgott  
Reg. No. 23,072

HELFGOTT & KARAS, P.C.  
60th FLOOR  
EMPIRE STATE BUILDING  
NEW YORK, NY 10118  
DOCKET NO.: FUJO 17.290  
BHU:priority

Filed Via Express Mail  
Rec. No.: EL522394475US  
On: February 5, 2001  
By: Brendy Lynn Belony  
Any fee due as a result of this paper,  
not covered by an enclosed check may be  
charged on Deposit Acct. No. 08-1634.



日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 2月 9日

出 願 番 号

Application Number:

特願2000-032372

出 願 人

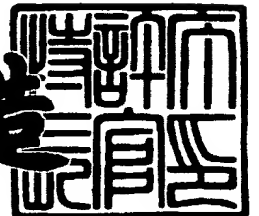
Applicant(s):

富士通株式会社

2000年10月 6日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2000-3082679

【書類名】 特許願

【整理番号】 9951776

【提出日】 平成12年 2月 9日

【あて先】 特許庁長官殿

【国際特許分類】 H04B 3/00

【発明の名称】 モバイル通信システム及びその方法

【請求項の数】 22

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 五十嵐 洋一郎

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 掛水 光明

【発明者】

    【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号 富士通九州通信システム株式会社内

    【氏名】 山村 新也

【発明者】

    【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号 富士通九州通信システム株式会社内

    【氏名】 村田 一徳

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 若本 雅晶

【特許出願人】

    【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100074099

【住所又は居所】 東京都千代田区二番町 8 番地 2 0 二番町ビル 3 F

【弁理士】

【氏名又は名称】 大菅 義之

【電話番号】 03-3238-0031

【選任した代理人】

【識別番号】 100067987

【住所又は居所】 神奈川県横浜市鶴見区北寺尾 7 - 2 5 - 2 8 - 5 0 3

【弁理士】

【氏名又は名称】 久木元 彰

【電話番号】 045-573-3683

【手数料の表示】

【予納台帳番号】 012542

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705047

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 モバイル通信システム及びその方法

【特許請求の範囲】

【請求項 1】 複数のサブネットワークからなるネットワークに接続する移動端末が、第 1 のサブネットワークから第 2 のサブネットワークに移動した後も、第 1 のサブネットワークにいた時と同様の通信を第 2 のサブネットワークにおいて行うことを可能とするモバイル通信システムにおいて、

該移動端末と通信を行う対応端末と、

該対応端末の認証を行う認証手段と、

該移動端末が該第 1 のサブネットワークから該第 2 のサブネットワークに移動した際に、該対応端末が該移動端末と通信を行うために必要な通信パラメータを設定する設定手段と、

該通信パラメータの設定のために該ネットワーク制御装置間で通信を行う通信手段と、

を備えることを特徴とするモバイル通信システム。

【請求項 2】 前記モバイル通信システムは、Mobile IP をプロトコルとして採用していることを特徴とする請求項 1 に記載のモバイル通信システム。

【請求項 3】 前記対応端末は、Mobile IP プロトコルをサポートしていないことを特徴とする請求項 2 に記載のモバイル通信システム。

【請求項 4】 前記対応端末が前記第 2 のサブネットワークに位置し、前記移動端末が前記第 1 のサブネットワークに位置する場合、

更に、該対応端末からのデータパケットを直接該第 1 のサブネットワークに送信し、該移動端末に着信させるトンネリング手段を備えることを特徴とする請求項 2 に記載のモバイル通信システム。

【請求項 5】 前記対応端末は、移動可能端末であることを特徴とする請求項 1 に記載のモバイル通信システム。

【請求項 6】 前記設定手段と、前記通信手段は、前記対応端末の隣接ルータに設けられることを特徴とする請求項 1 に記載のモバイル通信システム。

【請求項 7】 更に、前記対応端末が所定の領域に存在するか否かを判断する

在圏確認手段を備えることを特徴とする請求項 2 に記載のモバイル通信システム。

【請求項 8】前記対応端末が所定の領域に存在しないと判断された場合には、該対応端末に関連する前記通信パラメータを消去することを特徴とする請求項 7 に記載のモバイル通信システム。

【請求項 9】前記対応端末が Mobile IP 対応端末である場合、該対応端末と通信を行う前記移動端末が前記第 2 のネットワークへの登録を行わなくなったときに、前記対応端末が所定の領域外へ移動したと判断することを特徴とする請求項 2 に記載のモバイル通信システム。

【請求項 10】前記在圏確認手段は、前記対応端末に関連するパケットの送受信が行われなくなったことをもって、該対応端末が所定の領域に存在しなくなったと判断することを特徴とする請求項 7 に記載のモバイル通信システム。

【請求項 11】複数のサブネットワークからなるネットワークに接続する移動端末が、第 1 のサブネットワークから第 2 のサブネットワークに移動した後も、第 1 のサブネットワークにいた時と同様の通信を第 2 のサブネットワークにおいて行うことを可能とする、該移動端末と通信を行う対応端末を有するネットワークにおけるモバイル通信方法であって、

(a) 該対応端末の認証を行うステップと、

(b) 該移動端末が該第 1 のサブネットワークから該第 2 のサブネットワークに移動した際に、該対応端末が該移動端末と通信を行うために必要な通信パラメータを設定するステップと、

(c) 該通信パラメータの設定のために該ネットワーク制御装置間で通信を行うステップと、

を備えることを特徴とするモバイル通信方法。

【請求項 12】前記モバイル通信方法は、Mobile IP をプロトコルとして採用していることを特徴とする請求項 11 に記載のモバイル通信方法。

【請求項 13】前記対応端末は、Mobile IP プロトコルをサポートしていないことを特徴とする請求項 12 に記載のモバイル通信方法。

【請求項 14】前記対応端末が前記第 2 のサブネットワークに位置し、前記

移動端末が前記第 1 のサブネットワークに位置する場合、

更に、該対応端末からのデータパケットを直接該第 1 のサブネットワークに送信し、該移動端末に着信させるステップを備えることを特徴とする請求項 1 2 に記載のモバイル通信方法。

【請求項 1 5】前記対応端末は、移動可能端末であることを特徴とする請求項 1 1 に記載のモバイル通信方法。

【請求項 1 6】前記ステップ (b) 及び (c) は、前記対応端末の隣接ルータにおいて実行されることを特徴とする請求項 1 1 に記載のモバイル通信方法。

【請求項 1 7】更に、前記対応端末が所定の領域に存在するか否かの在圏確認を行うステップを備えることを特徴とする請求項 1 2 に記載のモバイル通信方法。

【請求項 1 8】前記対応端末が所定の領域に存在しないと判断された場合には、該対応端末に関連する前記通信パラメータを消去することを特徴とする請求項 1 7 に記載のモバイル通信方法。

【請求項 1 9】前記対応端末が Mobile IP 対応端末である場合、該対応端末と通信を行う前記移動端末が前記第 2 のネットワークへの登録を行わなくなったときに、前記対応端末が所定の領域外へ移動したと判断することを特徴とする請求項 1 2 に記載のモバイル通信方法。

【請求項 2 0】前記在圏確認ステップは、前記対応端末に関連するパケットの送受信が行われなくなったことをもって、該対応端末が所定の領域に存在しなくなったと判断することを特徴とする請求項 1 7 に記載のモバイル通信方法。

【請求項 2 1】移動端末と通信を行う端末を収容し、前記移動端末のホームエージェントから前記端末へ転送されてくる前記移動端末に関する結合情報をハントし、前記端末から移動端末に対するデータパケットを前記結合情報に基づいて処理することを特徴とするルータ。

【請求項 2 2】前記結合情報は、前記移動端末の IP アドレスと、フォーリンエージェントの IP アドレスを対応付ける情報であり、前記結合情報に基づいて前記端末から前記移動端末に対するデータパケットに対してトンネリング化処理を行うことを特徴とした請求項 2 1 に記載のルータ。



【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、モバイル通信システムに関し、特に、サブネットワーク間を移動する移動端末（モバイルノード：携帯PC等）を収容可能なネットワークに関する。

【0002】

【従来技術】

今日、インターネットの急速な発展により、IPパケットトラフィックが急増している。更に、携帯電話の普及に伴い、International Mobile Telecommunications 2000 (IMT-2000) での標準化も行われ、モバイル環境での高速IP通信が普及すると考えられる。このような急速な技術革新に関わらず、IP通信の高度化、すなわち、端末毎のQoS (Quality of Service)、WWWサーバ (World Wide Webサーバ) のネットワーク全体にわたる負荷分散といった付加価値サービスを実現する技術は、需要が見込まれる中で十分に成熟しているとは言えない。

【0003】

Cisco、3comなどの米ベンダが中心になって、PBN (Policy-Based Networking) という概念をIPネットワークを制御する枠組みとして提案している。PBNでは、ポリシーサーバがネットワークの運用ポリシー（ユーザにサービスを提供するために使用するデータ）をネットワーク機器群に設定し、ネットワーク機器群が、このポリシーを参照することで、QoS等のサービスを実現する。しかし、移動端末毎のポリシー設定（移動端末毎に提供するサービスを設定すること）を考えると、ポリシー追加／変更時、移動端末を収容する可能性のある全てのネットワーク機器群へのポリシーの設定が必要となり、ネットワーク全体でのポリシー設定処理量が増加する。更に、PBNで通知される情報をモバイルIP等の個々の移動端末に規定される基本サービスに適用するためには、それぞれのサービスに適用させるための仕様化と実装検討が必要であった。

【0004】

図25は、従来技術のポリシー (Policy) によるネットワークにおける品質制御の例を示す図である。

## 【0005】

ポリシーサーバ&NMS (NetWare Management System) がユーザとの間でサービス交渉を行い、ユーザ単位でのアドミッション制御を固定網において提供する「ポリシーベースネットワーク：PBN」のような方法が検討されている。PBNでは、ポリシーサーバがネットワークの運用ポリシー (制御パラメータ) をネットワーク機器群 (ルータなど) に配布設定し、ネットワーク機器群が、パケット制御時に、前述のポリシーを参照することでQoS (Quality of Service：サービス品質制御) 等のサービスを実現する。

## 【0006】

しかし、移動端末個々に対して「専用の」ポリシー設定をしようとした場合、問題が生じる。それは、ポリシー追加／変更時、移動端末の送受するパケットを中継する可能性のあるすべてのネットワーク機器群へポリシーの設定をすることが必要となり、ネットワーク全体でのポリシー設定処理量が莫大に増加する。言い換えると、各ルータなどのネットワーク機器群は、莫大な数の「端末毎のポリシーデータ」を保持しなくてはならないことになる。端末毎のサービス制御方法としては、これは現実的ではない。

## 【0007】

## 【発明が解決しようとする課題】

音声とデータ通信が統合された、多様な種類の端末が接続されるIPネットワークでは、遅延に敏感なトラフィックやビジネス上優先度の高いトラフィックを保護するため、QoSを実現する手段として、Int-Serv (RSVP：RFC2205参照) やDiff-Serv (RFC2475参照) といった方式が提案されているが、キャリア網やバックボーン網 (インターネットの主ネットワーク接続網) としてはオーバーヘッドが少ないDiff-Serv方式が有力視されている。しかし、Diff-Servは、経路上のネットワーク機器へのポリシー設定を必要とし、Diff-Serv単独ではネットワーク管理が煩雑になるといった問題がある。

## 【0008】

そのためネットワーク機器へのポリシー設定をポリシーサーバと呼ばれるサーバから一括設定する PBN (Policy-Base Networking) という概念が提案された。しかし、移動端末をサポートした様々なプロバイダ、キャリアから構成されるシームレスな (seamless: 継ぎ目のない) グローバルネットワークでは、全てのローカルネットワークが接続可能性のあるユーザに対するポリシーの決定とネットワーク機器への情報設定が可能でなければならない。PBNでこれを行うためには、全てのユーザのポリシー情報をローカルに保持するか、可能性のある全てのネットワーク機器に対して情報を予め設定するしかない。

## 【 0 0 0 9 】

これは億単位にも上るユーザに対して実行するのは極めて非効率的であり、現実的ではない。また、全てのユーザのポリシー情報を常時、ネットワーク機器に保持するのは、ネットワーク機器のメモリ量増加を招き、これら膨大な情報を処理するための負荷が大きくなって処理能力を劣化させる。

## 【 0 0 1 0 】

逆に、常にポリシーサーバへ尋ねるような処理方式とする場合は、ポリシーサーバへの問い合わせのオーバヘッドが発生し、SLA (Service level Agreement) を遵守できない可能性が増大するといった問題もある。

## 【 0 0 1 1 】

本発明の課題は、移動端末を広範にサポートするネットワークの通信システムを提供することである。

## 【 0 0 1 2 】

## 【課題を解決するための手段】

本発明のモバイル通信システムは、複数のサブネットワークからなるネットワークに接続する移動端末が、第1のサブネットワークから第2のサブネットワークに移動した後も、第1のサブネットワークにいた時と同様の通信を第2のサブネットワークにおいて行うことを可能とするモバイル通信システムにおいて、該移動端末と通信を行う対応端末と、該対応端末の認証を行う認証手段と、該移動端末が該第1のサブネットワークから該第2のサブネットワークに移動した際に、該対応端末が該移動端末と通信を行うために必要な通信パラメータを設定する

設定手段と、該通信パラメータの設定のために該ネットワーク制御装置間で通信を行う通信手段とを備えることを特徴とする。

## 【 0 0 1 3 】

本発明のモバイル通信方法は、複数のサブネットワークからなるネットワークに接続する移動端末が、第 1 のサブネットワークから第 2 のサブネットワークに移動した後も、第 1 のサブネットワークにいた時と同様の通信を第 2 のサブネットワークにおいて行うことを可能とする、該移動端末と通信を行う対応端末を有するネットワークにおけるモバイル通信方法であって、(a) 該対応端末の認証を行うステップと、(b) 該移動端末が該第 1 のサブネットワークから該第 2 のサブネットワークに移動した際に、該対応端末が該移動端末と通信を行うために必要な通信パラメータを設定するステップと、(c) 該通信パラメータの設定のために該ネットワーク制御装置間で通信を行うステップとを備えることを特徴とする。

## 【 0 0 1 4 】

本発明のルータは、移動端末と通信を行う端末を収容し、前記移動端末のホームエージェントから前記端末へ転送されてくる前記移動端末に関する結合情報をハントし、前記端末から移動端末に対するデータパケットを前記結合情報に基づいて処理することを特徴とする。

## 【 0 0 1 5 】

本発明によれば、サブネットワーク間を移動する移動端末と対応端末がサブネットワーク間をまたいで通信する場合に必要な通信パラメータの管理や通信パラメータの設定のための通信を、ネットワーク内に設けた装置によって行い、対応端末は、これらの装置を介して移動端末と通信を行うようにする。従って、対応端末は、移動端末との通信サービスを受ける上で、特別な機能を有する必要はなく、対応端末に多くの処理負荷を課すことがない。よって、対応端末としては、ユーザの有する様々な端末が使用可能であり、ユーザは、容易に、移動端末との通信サービスを受けることが出来る。

## 【 0 0 1 6 】

## 【発明の実施の形態】

本発明では、本出願人が先に出願した特願平 1 1 - 2 7 6 7 0 3 号に記載された技術を前提に考える。以下には、同出願の内容を簡単に説明するが、詳細は、同出願に含まれる明細書を参照いただきたい。

## 【 0 0 1 7 】

同出願では、R F C 2 0 0 2 で規定されている Mobile IP と、現在 IETF (Internet Engineering Task Force: インターネットに関する主な標準化組織) で検討中の A A A (Authentication, Authorization and Accounting) システムと、の連携による Mobile IP アーキテクチャをベースにした、集中管理されたユーザのプロファイルからプロバイダ間をまたがるグローバルなネットワークへ効果的に必要な情報 (ポリシー) を設定するサービス制御の枠組みを提供する。

## 【 0 0 1 8 】

A A A システムにネットワーク機器に設定する情報をユーザ単位に保持するデータベースを設け、認証要求時に該ユーザのユーザ識別子 (N A I : Network Access Identifier) から情報を抽出し、R F C 2 0 0 2 で規定された機能エンティティ、F A (Foreign Agent、詳細は後述)、H A (Home Agent、詳細は後述) が必要とする情報を選別して通知する機能を追加する。また、機能エンティティ間の通信に用いるプロトコルを各エンティティが必要とする情報を通知出来るように拡張し、H A と F A に A A A システムから通知された情報をキャッシュする機能を持たせ、ネットワーク機器への情報設定とパケット編集の制御機能を追加する。これらの機能を Mobile IP の登録手順と移動に伴うハンドオフ (ハンドオーバー) や、ルートの最適化手順と連携させることにより、ユーザがネットワークにアクセスしている間のみ有効なポリシー情報を設定することが可能となる。

## 【 0 0 1 9 】

従って、本発明に於いては、Mobile IP を前提に説明を行うが、Mobile IP の詳細については、以下の参考文献を参照されたい。

## 【 0 0 2 0 】

「詳解 Mobile IP 移動ノードからのインターネットアクセス」 ジェイムズ、D、ソロモン著、寺岡文夫 + 井上淳 監訳、出版 - ピアソンエデュケーション

ン社

以下に、実施形態の説明に登場する略称について説明する。

- ・ M I P (Mobile IP)

R F C 2 0 0 2 と将来の全ての拡張で規定される Mobile IP プロトコル。

- ・ A A A プロトコル

A A A システムが使用するプロトコル。本発明では、使用するプロトコルを特定しないが、実施形態では現在 IETF で検討中の D I A M E T E R プロトコル（現在最も多くインターネット・サービス・プロバイダによって使用されている認証、課金のためのプロトコル R A D I U S を拡張したもので、現在 IETF において検討されている）の使用を想定する。A A A プロトコルは認証、認可、課金、ポリシーに関する情報を伝達可能なあらゆるプロトコルで実装可能である。

- ・ データベース検索プロトコル

サービスプロファイルデータベースを検索するためのプロトコル。使用するプロトコルはサービスプロファイルデータベースを実装するデータベースの製品に依存する。L D A P (Lightweight Directory Access Protocol: International Standard Organization (I S O) 及び International Telecommunication Union (I T U) の標準である X. 5 0 0 に規定されている) が通常用いられる。本発明では、検索プロトコルとデータベースの動作については言及しない。

- ・ M N (Mobile Node)

Mobile IP プロトコル機能を有する移動端末。

- ・ C N (Correspondent Node)

移動端末が通信を行う、通信ノード。

- ・ A A A

Authentication (認証)、Authorization (認可)、Accounting (課金) を行うサーバ群の IETF で用いられる名称。H A へ H A 登録要求 (H A R : Home Agent Registration) で Foreign Agent (F A) へは、A A A F を経由した認証応答 (A M A : Authentication Message Acknowledge) でサービスプロファイルを通知する機能を有する。

## 【 0 0 2 1 】

本発明の A A A は上記機能に加え、サービス制御データベースから認証要求ユーザのサービスプロファイルを抽出し、パケット制御情報が設定可能な汎用フォーマットを持つサービスプロファイルを生成するサービス管理機能を持つ。A A A H は認証要求ユーザの加入者データを持つネットワークの A A A であり、A A A F は該ユーザの加入者データを持たないネットワークの A A A である。A A A F はユーザの N A I (Network Access Identifier) より A A A H を特定し、F A と A A A H 間のメッセージ交換を代理する。

## ・ F A (Foreign Agent)

R F C 2 0 0 2 で定義される機能エンティティ。移動端末に割り付けられるホームアドレスを所有しないエージェントであり、自ノードのアドレスである気付アドレス (Care-of-Address) へカプセル化されて送出してきたパケットをデカプセル化し、ホームアドレスに対応したリンクレイヤアドレスへパケットを中継 (Relay) する。このアドレスの対応は、訪問者リストと呼ばれるテーブルで管理される。F A は移動端末のアクセスルータと A A A プロトコルクライアントでもある。F A は D I A M E T E R セッションを管理するセッションランザクションを持つ。

## ・ H A (Home Agent)

R F C 2 0 0 2 で定義される機能エンティティ。移動端末に割り付けられたホームアドレスを所有するエージェントであり、H A に中継されてきた移動端末のホームアドレスを送信先とするパケットはホームアドレスに対応した F A の気付アドレス (Care-of-Address) へカプセル化されて送出される。ここで、気付アドレスとは、通常の郵便システムにおける私書箱のようなものである。このアドレスの対応は、(移動性) 結合キャッシュと呼ばれるテーブルで管理される。H A は A A A プロトコルクライアントでもある。H A は D I A M E T E R セッションを管理するセッションランザクションを持つ。

## 【 0 0 2 2 】

更に、本発明は、Mobile IPにおける経路最適化及び、特願平 1 1 - 2 7 6 7 0 3 号の技術に関連する。

## 【 0 0 2 3 】

図 1 は、Mobile IP を説明する図である。

## 【 0 0 2 4 】

ネットワークは、サブネットワーク 1 と 2 から構成されているとする。移動ノード (MN) 1 2 がサブネットワーク 2 に最初において、HA 1 1 を介して CN 1 3 と通信をしていたとする。MN 1 2 は、携帯 PC などのように持ち運んで、異なるネットワークに接続可能である。

## 【 0 0 2 5 】

ここで、MN 1 2 がサブネットワーク 2 からサブネットワーク 1 に移動したとする。MN 1 2 は、サブネットワーク 1 に移動して、サブネットワーク 2 に接続されている CN 1 3 と通信を始めようとする。最初に、MN 1 2 は、サブネットワーク 1 の FA 1 0 に対し、自分がサブネットワーク 1 に来たことを登録してもらうため、登録申請を FA 1 0 に対して行う。また、FA 1 0 は、MN 1 2 が FA 1 0 の配下に入ったことをサブネットワーク 2 の HA 1 1 に通知する。HA 1 1 は、FA 1 0 からの通知を元に、CN 1 3 に対し、MN 1 2 と通信するためのネットワークの結合情報の更新指示を出す。HA 1 1 は、MN に関する登録が完了するとその応答を FA 1 0 に送信する。FA 1 0 は、MN 1 2 からの登録申請に基づいて、MN 1 2 が FA 1 0 の配下に入ったことを登録すると、通信が可能である旨の通知として、MN 1 2 に返答メッセージを送信する。CN 1 3 は、更新指示に基づいて、MN 1 2 へメッセージを送る場合には、FA 1 0 に宛てて信号を送信し (トンネリング)、FA 1 0 に MN 1 2 へのメッセージを転送してもらうことにより、MN 1 2 への通信を可能とする。

## 【 0 0 2 6 】

また、MN 1 2 から CN 1 3 に宛てた通信は、まず、MN 1 2 が CN 1 3 を宛先として指定したメッセージを FA 1 0 に送る。FA 1 0 は、MN 1 2 から受け取ったメッセージを直接 CN 1 3 に送信する。このようにすることによって、MN 1 2 がサブネットワーク 1 に移動した後も、CN 1 3 との通信を行うことが出来る。

## 【 0 0 2 7 】



図 2 は、図 1 の通信経路を抜き出した模式図である。同図 (a) は、経路最適化のない場合を示し、同図 (b) は、経路最適化がある場合を示している。

## 【 0 0 2 8 】

図 2 (a) に示すように、経路最適化がない場合には、MN から送信されたメッセージは、FA に送られ、FA から CN に送信される一方、CN からのメッセージは、一旦、HA に送られてから、FA に送信され、FA から MN に送信される。このように、CN から MN のメッセージは、一旦 HA を通らなくてはならないので、ネットワークリソースである HA の機能を通信毎に利用することになり、ネットワークリソースの無駄使いが生じている。

## 【 0 0 2 9 】

図 2 (b) は、経路最適化が行われた場合であり、経路最適化機能を有する CN は、MN 宛のメッセージを HA ではなく、FA に直接送信し、MN まで送る。MN から CN へのメッセージの流れは図 2 (a) と同様である。このようにすることにより、通信の度に HA を介さなくて良くなるので、ネットワークリソースの無駄使いを防止することが出来る。

## 【 0 0 3 0 】

機能 (1) Mobile IP における経路最適化 (draft-ietf-mobile ip-optim-08.txt) は、Mobile IP における HA が持つ結合キャッシュ管理機能、トンネルパケット作成機能を CN が装備することで、個々の CN が MN の気付アドレスを宛先としたトンネルパケットを作成、送信する。この結果、MN と通信する個々の CN のパケットは、HA を経由せずに直接 MN の気付アドレスに対してトンネリングによって送付される。この場合、各 CN は、経路最適化に必要なプロトコル操作の能力、及び、CN 単位に保持すべきデータを自身で管理しなければならない。

## 【 0 0 3 1 】

機能 (2) 特願平 1 1 - 2 7 6 7 0 3 号の技術では、各 CN 毎に個別サービス制御を施すために、各 CN に対して「サービスプロファイル」を配布する。具体的には、経路最適化で使用する結合更新メッセージにサービスプロファイルを付加して、これを CN に送付する。CN は、上述の結合キャッシュの場合と類似

して、自身の中に受信した結合キャッシュに関するエントリが無い場合はこれを新規に作成し、既にエントリが存在する場合は、該サービスプロファイルが更新される。

## 【 0 0 3 2 】

このように、個別サービス制御を実施するためのCNへの要求条件として、個々のCNに対して機能追加が必要であった。CNは、特願平11-276703号の個別サービス制御を受けるためには、上述の機能(2)を搭載することが必須条件であった。

## 【 0 0 3 3 】

更に、特願平11-276703号におけるCNの前提条件として、同特許出願の個別サービス制御を受けることのできる移動端末はMobile IPの処理能力が必須とされる。これは、移動端末におけるISP (Internet Service Provider) へのアクセスに主要なプロトコルであるPPP (Point-to-Point Protocol) によるダイヤルアップ接続を始めとして、一部のリンクレイヤに対応できない。このため、可搬性のあるCN (移動端末) が特願平11-276703号の個別サービス制御を受けることが不可能であった。これについては、実現に際して以下の課題があった。

(1) 特願平11-276703号のサービス対象となるために、CNは機能追加を要求される。処理能力の低い機器に対しての機能追加は、処理能力上の負荷を増大させることになる。処理能力に余裕のある、据え置き型ワークステーション、PCにおいては、問題にならないが、小型のモバイル機器においては、同機能追加は深刻な問題となる場合がある。

(2) 同様に、特願平11-276703号においては、同技術の提供する個別サービス制御を享受するために、CNに機能追加が必須となる。これは、同アーキテクチャのサービスを普及させる上で障害となる。あらゆるCNが同一サービスを享受するためには、端末への個別の要求条件が無いことが必要である。

(3) 更に、リンクレイヤ種別に依存する機能制限によりCNからISPへの接続形態でMobile IPを利用できない移動端末においても、ネットワーク側で機能代行することで個別サービス制御を提供できることが必要である。特に、ネット

ワーク間の移動を前提としたCNの利用形態の多くは、ダイヤルアップPPPであり、Mobile IPが利用できない。(2)と同様、サービス普及の障害となりうる。

## 【 0 0 3 4 】

従って、特願平11-276703号におけるCNでは、実装を考慮すると、特に移動型CNに対する障害が大きく、同アーキテクチャ固有機能の追加を要求している。同サービスを広範囲の端末種別、ユーザ種別に対して提供するために、CNの機能をネットワーク側に収容することで、以下の二点を実現することが、広範なサービス普及のために必須である。

(1) 個々のCNを機能追加から解放すること。

(2) 非Mobile IP環境下の移動端末についても、個別サービス制御を受けられること。

## 【 0 0 3 5 】

図3は、本発明の一実施形態のネットワーク構成を示す図である。

## 【 0 0 3 6 】

本発明の実施形態に於いては、上記で説明したように、CNに多くの機能増加を負担させるのではなく、ネットワークにCNの機能を代理させるプロキシCNを設ける。全体のネットワークは、Mobile IPネットワーク20によって構成され、前述したMN、FA、AAAF、AAAH、HAが設けられ、FA、HA、AAAF、AAAHは、IP転送網21によってメッセージの交換が可能となっている。

## 【 0 0 3 7 】

すなわち、MNがHAに収容されるCNと通信したい場合、FAに登録申請を行う。これは、AAAFを介してAAAHに通知される。AAAHは、サービスプロファイルデータベース22を参照して、サービス提供内容を確認し、HAに通知する。ここで、上記説明では、HAに直接CNが接続され、MNと通信することを述べた。しかし、この方法では、CNの機能増大が大きくなり、CNもMNと同様な携帯PCの場合、プロセッサの処理容量が足りず、処理遅延を生じる可能性がある。

## 【0038】

従って、CN25とHA26の間にプロキシCN24を設ける。プロキシCN24は、後述するCMF、TCF、MHF、CD、MAFという機能群を備えている。CN25は、MNと通信するためにプロキシCN24にアクセスする。プロキシCN24は、リンクレイヤ認証サーバ23にCN25のアクセスを認証するか否かを問い合わせる。リンクレイヤ認証サーバ25は、CN25のNAIより、サービスプロファイルデータベース27を参照して必要なパラメータを取得し、CN25に提供するサービス内容を確認して、プロキシCN24に許可通知を行う。プロキシCN24では、CN25が認証されたことを受けて、CN25に通信許可を出す。通信許可を受けたCN25は、プロキシCN24及びHA26を経由してCN25からのメッセージをMNに送信する。HA26に送られたメッセージは、前述したとおり、MNに送信される。

## 【0039】

このように、CN25に設けるべき機能をプロキシCN24に設けたことにより、個々のCNは、機能増加を行う必要が無く、どのようなCNであっても当該ネットワークのサービスを受けることが出来る。

## 【0040】

また、CN25に提供されるサービスがトンネリングを含む場合、CN25からプロキシCN24に渡されたメッセージは、直接FAに送られる。

## 【0041】

同図のサービスプロファイルデータベース27は、ユーザ識別子（NAI）単位のサービスプロファイルから構成される。サービスは、セキュリティ、マルチキャストなどを含む多様なサービスを登録、実現可能である。

## 【0042】

サービスプロファイルはユーザを識別するためのNAIとサービス種別により異なる構成を持つサービスブロックから構成される。サービスブロックはサービスタイプ、ポリシー、サービス固有情報から構成される。パケットフィルタリングのサービス固有情報は、規制アドレスと適用条件である。移動端末の送信パケットに適用されるDiff-Serv送信のサービス固有情報は受信先アドレス、受信先

ポート、T O S (Type of Service) 値である。移動端末の受信パケットに適用されるDiff-Serv受信のサービス固有情報は送信元アドレス、送信元ポート、T O S 値である。

【 0 0 4 3 】

ここで、図 4 に、サービスプロファイルの例を示す。

【 0 0 4 4 】

サービスプロファイルは、本発明が提供する I P サービス制御を実行するために必要な、パケット制御の手段を記述した「情報セット」である。

【 0 0 4 5 】

具体的な項目としては以下の構成要素がある。

( 1 ) 制御対象パケット情報

具体的に制御を加えるパケット種別を特定する情報

( 2 ) ルーティング／パケット編集情報

パケット制御の種別、手段に関する情報（例：転送先アドレス等）

( 3 ) 個別制御情報

物理装置に個別のサービス制御の手段に関する情報

F A と H A はルータ制御部とサービス制御部から構成される。

【 0 0 4 6 】

ルータ制御部は、ルーティングテーブル、一時的なルーティングテーブルである結合キャッシュ、サービス制御対象パケットを特定するサービス制御フィルタを有し、受信 I P ヘッダ抽出とヘッダ情報の編集機能を有する。

【 0 0 4 7 】

サービス制御部は、サービス制御トランザクションを有し、ルータ制御部からの要求に従い、サービス制御トランザクションの設定、検索、更新、削除を行う。サービス制御部は、M I P、D I A M E T E R プロトコルを実装し、メッセージ受信バッファ、メッセージ送信バッファを備えた一般的なプロトコル処理機能も有する。

【 0 0 4 8 】

プロキシ C N 機能群は、各 C N に実装が必要であった機能を、C N から分離し

、ネットワーク側に配備する場合に必要な機能エンティティの集合である。

【0049】

具体的には、以下に挙げる機能群により構成される。各機能群を以下のように定義する。

(1) CMF : Cache Management Function Mobile IPにおける経路最適化に関する結合キャッシュ（通信相手の移動ノード（以下、MN）の気付アドレス等）を格納、管理する。具体的には、HAから送付される結合キャッシュを検出し、このキャッシュに関するエントリが無い場合は新規に生成し、更に既存のキャッシュが存在する場合は、受信した結合キャッシュの情報で更新する。

(2) TCF : Tunneling Capability Function、上記に関連し、経路最適化を実現するMNの気付アドレスへのトンネルパケットを生成する機能。MNに対してパケットを送信しようとする場合、本機能を装備する場合、送信パケットをカプセル化（例：IP-in-IPカプセル化）し、結合キャッシュに格納される、宛先情報に基づき、カプセル化を行う。

(3) MHF : Message Handling Function、本発明において個別のメッセージインターフェースを定義する場合、このメッセージの送受信を行う。プロキシCN機能群が分散した物理エンティティに配備され、相互に独自の情報交換を行う必要がある場合、送信側におけるメッセージ生成、受信側におけるメッセージ検出を行う。

(4) MAF : Mobile Agent Function、Mobile IPにおける移動性エージェント機能。Mobile IPを利用可能なCNのプロキシCNへの動的な登録、削除において利用される。

(5) CD : Cache Data、本発明の実施形態において、本来CNが持っているべきデータベースの内容であって、これを格納しておくメモリ等を有している。具体的には、訪問者リストと結合キャッシュとからなる。

【0050】

プロキシCNが、個々のCNの登録管理のために必要なデータを以下に挙げる。

(1) 訪問者リスト (Visitor List) : Mobile IPのFAが保持する訪問者リ

ストを基本に、CN毎の在圏状態フラグ、及び、後述のキャッシュデータへの関連付けをするための情報（ポインタ）を拡張している。

（２）結合キャッシュ：Mobile IPにおける経路最適化における、従来、CNが保持すべき結合キャッシュ。

（３）サービスプロファイル：特願平 1 1 - 2 7 6 7 0 3 号における、NAI 毎に用意される、個別サービス制御を実施するためのプロファイルデータ。

#### 【 0 0 5 1 】

以上、プロキシCNを構成する機能エンティティ、データは、実現方式によりネットワーク内の配備が変わるため、物理エンティティに対する固定的なマッピングは無い。換言すれば、これらの機能を全てプロキシCNに設ける必要はなく、これらの機能の一部をCNに持たせたり、HAに持たせることも可能である。

#### 【 0 0 5 2 】

図 5 は、プロキシCNへのCNの登録処理を示す図である。

#### 【 0 0 5 3 】

ネットワーク間を移動可能なCN（以下、移動CN）が在圏中のISPが管理するプロキシCNに登録する場合において、一般的なアクセス方法としてはPPP（Point-to-Point Protocol）があり、電話回線によるISPへの接続では多くの場合、同プロトコルを利用する。

#### 【 0 0 5 4 】

ところが、PPPを経由してISPの提供するプロキシCNを利用しようとする場合は、Mobile IPを認識できない。この理由として主には、Mobile IPの移動ノード（移動CN）がホームアドレスを指定して登録要求するが、PPPのダイヤルアップサーバは、このようなアドレス（在圏ネットワークとプレフィックスが異なるアドレス）を許容できない点がある。

#### 【 0 0 5 5 】

このようなケースにおいて、Mobile IPを使用せずにプロキシCNを利用する手段を提供する。

#### 【 0 0 5 6 】

PPP経由のCNの認証では、Mobile IPネットワークにおけるAAAサーバ

は利用できないため、代替としてPPP接続のCNに対してはリンクレイヤ認証サーバを別途用意し、PPP経由のCNに対しては同サーバの認証を持ってネットワークへの接続を許容する。

## 【0057】

また、本ケースに該当するCNに関するサービスプロファイルの配布方法としては、AAAサーバでなく、前述のリンクレイヤ認証サーバと連結したサービスプロファイルデータベース（サービスプロファイルDB）を用意し、ここに該当するCNに関するサービスプロファイルの元データを格納する。リンクレイヤ認証サーバは、CNからの接続要求を受け（図5の（1））、正当なCNであることを確認後、サービスプロファイルDBより、プロファイルデータを読み出し（図5の（2））、プロキシCNに通知する（図5の（3））。そして、リンクレイヤ認証サーバからCNに対し、アクセス許可を出力する（4）。

## 【0058】

これにより、PPPをはじめとするMobile IPを利用できないCNにおいても、プロキシCNへの登録手段を提供し、個別サービス制御を可能にする。

## 【0059】

あるいは、CNがMobile IPを利用できる場合、このCNのプロキシCNへの登録手段としては、Mobile IPの基本メカニズムである。MN（Mobile Node）がFA（Foreign Agent）に登録する手段を利用し、実現できる。プロキシCNには、移動性エージェントの機能（MAF：Mobile Agent Function）を持つので、Mobile IPの登録手順によりCNがプロキシCNに登録される。プロキシCNは、AAAサーバからHA経由で該CNに関するサービスプロファイルの配布を受け、プロキシCN内で、管理する該CNに関するサービスプロファイルキャッシュに保持する。

## 【0060】

図6は、CNがプロキシCNに登録されるまでの基本的な手順を示すシーケンス図である。

## 【0061】

図6は、Mobile IPにおいて、移動ノード（MN：Mobile Node）が外部エー



ジェント（F A : Foreign Agent）に登録する際に送受されるメッセージと基本的に変わりない。差異は、プロキシCN内部処理として、登録したCNの結合キャッシュ、サービスプロファイルキャッシュのエリアを作成する機能がある、というものである。

（１）プロキシCNはMobile IPの外部エージェント（Foreign Agent : F A）の機能を兼ねている。よって、プロキシCNはF Aが実装しているエージェント広告メッセージを自らが属するサブネットワーク内に「ブロードキャスト」する。このブロードキャストは当該サブネットワーク内の全てのノードが受信する。プロキシCNは、自身に登録しようとするノードに受信させてプロキシCNの存在を知らせる。

（２）プロキシCNの配下にローミング（移動）してきたCNは、プロキシCNが発信するエージェント広告メッセージを探す。このメッセージを受信したCNは、プロキシCNに対して登録を要請するために、自CNの情報を含めた登録要求メッセージを構成する。

（３）前項で構成した「登録要求メッセージ」を送出する。宛先はプロキシCNとなる。

（４）プロキシCNは、登録要求メッセージを送信したCNの正当性を認証する。認証の方法は、実装依存であるが、A A Aサーバに認証を依頼する方法、また、CNのホームエージェントが認証する方法等がある。CNの正当性が認証されると、プロキシCNは次のステップに進む。

（５）プロキシCN独自の動作として、登録しようとするCNについて、サービスプロファイルキャッシュ、結合キャッシュを生成する。

（６）以上のステップが正常に終了したところで、プロキシCNはMobile IPの「登録応答」メッセージをCN宛に送信する。これを受信したCNは自らが発信した登録要求が正常に受理されることを知る。

【 0 0 6 2 】

図 7 は、プロキシCN内の個別サービス制御データの管理方法を示す図である。

【 0 0 6 3 】

プロキシCN内部の、管理対象のCNに関連するキャッシュデータを保持する手段について述べる。プロキシCNはMobile IPの移動性エージェント機能が持つ訪問者リスト (Visitor List) に関連付ける。訪問者リストには該プロキシCNの圏内に在圏する個々のCNに関する情報を保持している。具体的な関連付けの方法は、各々の訪問者リストエントリに拡張情報を付加し、この拡張部に結合キャッシュ、サービスプロファイルキャッシュの所在を示すインデックスポイントを格納する。これにより、プロキシCNが保持する結合キャッシュ、及びサービスプロファイルキャッシュの取り扱いは、移動性エージェント機能 (MAF) における訪問者リストの管理と連携することができ、キャッシュの生成、抹消等の処理が容易になる。ここで、結合キャッシュは、加入者であるCNにアクセスしてきたMNのアクセスするFAの気付アドレスと、MNのホームアドレスとを関連付けて記憶しているものである。

【0064】

図8、9は、CNの在圏管理方法の一実施形態を示すシーケンス図である。

【0065】

移動CNは、動的にプロキシCNに登録され、かつ、他ネットワークへ移動したことを検知するためには、個々のCNが該プロキシCN配下に在圏していることを定期的に確認する必要がある。

【0066】

この確認手段のうち、本実施形態は、該CNがMobile IPを利用してプロキシCNに登録されている場合である。

【0067】

該CNは登録手段としてMobile IPの登録手順に沿ってプロキシCNに登録されている。このMobile IPの登録時には、登録の有効期間 (Lifetime) が決定され、この有効期間が満了する前に再登録しなければならない。該CNがMobile IPを利用できる場合は、上述のMobile IPの周期的な再登録手順を在圏確認としても利用する。

【0068】

特定の加入者についての処理をフローチャートとして示したのが、図9である

## 【 0 0 6 9 】

図 9 において、ステップ S 1 において、登録有効期間の監視を開始し、ステップ S 2 において、上記テーブルの検索を行う。ステップ S 3 において、当該加入者の再登録によるタイムスタンプの書き換えが起きたことを検出したか否かを判断し、検出した場合には、ステップ S 1 に戻って再び監視を開始し、再登録が無かった場合には、ステップ S 4 において、当該加入者の登録を削除する。

## 【 0 0 7 0 】

図 1 0 ～ 1 2 は、CN の在圏管理方法の別の実施形態を示した図である。

## 【 0 0 7 1 】

図 8、9 の実施形態に対して、CN が Mobile IP を利用できない場合は、Mobile IP のような周期的かつ明示的な登録手段が存在せず、登録メッセージの有無で明示的に在圏、非在圏を確認することができない。この場合、周期的に在圏確認する一般的な手段は無いが、一定時間、該 CN のアクティビティ（パケット送信）が無かった場合に、圏外（他のネットワーク、ISP）へ移動したと判定することができる。確認の手段としては、以下の二種がある。

## 【 0 0 7 2 】

図 1 0 は、CN が Mobile IP を使用できない場合の在圏管理方法の第 1 の方法を示すフローチャートである。

## 【 0 0 7 3 】

前提となるデータとして、プロキシ CN は各 CN 毎に在圏状態を示すデータを保持する。ここでは在圏状態フラグ、と称する。

## 【 0 0 7 4 】

まず、通常、パケットを監視し（ステップ S 1 0）、該 CN の初期登録時、もしくはパケットを（頻繁に）送信していることが確認される間は、在圏フラグは「在圏」状態となっている。

## 【 0 0 7 5 】

次に、プロキシ CN は、該 CN からのパケットフローが一定期間無いことを検出すると（ステップ S 1 1）、該 CN が圏外へ移動している可能性を予想し、在

圏状態フラグを「保留」に変更する。

#### 【0076】

「保留」状態への移行と同時に、プロキシCNは判定用のタイマを起動し（ステップS12）、このタイマ満了までに該CNに関するパケットフローが無い場合（ステップS16）、該CNの状態として、「圏外へ移動している」と判定する。このときの在圏状態フラグは「圏外」となる（ステップS17）。一旦、「圏外」と判定されると、Mobile IPが使用可能な場合に周期的な再登録を受信しなくなった場合と同様、プロキシCNは、該CNに関する登録を抹消する（ステップS18）。この過程において、データエントリも削除される。ステップS14で、パケットを検出した場合には、ステップS15において、該CNの状態を「在圏」に変更して、ステップS10に戻り、パケットの監視を続ける。

#### 【0077】

図12は、図10の方法における在圏フラグの状態遷移の様子を示した図である。

#### 【0078】

最初在圏状態にあった在圏フラグは、パケットフローが消失した時点で、保留状態になる。ここで、再びパケットフローが検出できた場合には、在圏フラグは、在圏状態に戻る。しかし、保留状態に於いて、更に、パケットフローが検出できない場合には、CNはプロキシCNの圏外に出たと判断し、在圏フラグの状態を圏外状態とする。新規に登録するCNは、データエントリが作成された後、在圏フラグが最初に在圏状態に設定され、その後は、上記したような遷移をCNが圏外に出てしまうまで繰り返す。

#### 【0079】

図11は、CNがMobile IPを使用できない場合の在圏管理方法の第2の方法を示すフローチャートである。

#### 【0080】

プロキシCNが管理している各CNについて、訪問者リストエントリの拡張データとして、「前回の在圏確認時刻」（以下、確認タイムスタンプ）を追加する。また、プロキシCN全体で単一の周期的な監視タスク（以下、監視タスク）を

起動しておく。

【 0 0 8 1 】

前述の監視タスクは、一定の周期にて在圏する全CNの確認タイムスタンプを参照する。確認タイムスタンプとは、前回周期に該CNから発信するパケットを検出した時刻である。

【 0 0 8 2 】

このとき、現在時刻と確認スタンプとの時間差が、プロキシCN内で規定される基準値よりも大きい場合、すなわち一定期間以上、CNからのパケットフローが無い場合には、該CNの登録を抹消する。規定値以内であれば、在圏すると認識され、プロキシCNは登録された状態を保持する。

【 0 0 8 3 】

すなわち、図 1 1 においては、ステップ S 2 0 において、在圏確認を開始し、監視タスクが処理を始める。まず、ステップ S 2 1 において、第 n 番目の CN エントリが検索される。そして、ステップ S 2 2 において、該 CN の前回のパケット検出時刻との比較を行う。このとき、検出時刻は、確認タイムスタンプを読み込むことによって取得する。そして、ステップ S 2 3 において、前回確認時刻と比較し、時間差が規定値以内か否かが判断される。時間差が規定値以内であれば、ステップ S 2 4 において、最新のパケットを検出し、検出されれば、その時刻を確認タイムスタンプに登録する。また、ステップ S 2 3 において、時間差が規定値外であれば、CN の登録を抹消する。監視タスクはステップ S 2 1 からステップ S 2 5 を全ての CN のエントリについて行い、ステップ S 2 6 において、一監視周期の終了が確認され、ステップ S 2 0 に戻って、再び在圏確認処理を再開する。

【 0 0 8 4 】

また、他の CN の在圏管理方法として、以下のようなものがある。

【 0 0 8 5 】

Mobile IP を利用できない CN において、CN が明示的に電話回線の切断等にて、プロキシ CN とのリンクを切断する場合は考えられる。これはプロキシ CN 側（ネットワーク側）では、リンクレイヤの回線切断として検出できる。プロキ

シCNは、このリンクレイヤの切断に関する情報を監視し、切断を検出した場合、該CNの圏外への移動と判定し、該CNの登録抹消の処理を実行する。

## 【 0 0 8 6 】

このように、リンクレイヤの回線断としてプロキシCNとCNとのリンクの切断を検出するための具体的手法については、当業者によれば容易に理解されるであろう。従って、CNの圏外への移動判断と、これに基づいた登録の抹消処理の実現も当業者によれば容易に実現されるものとする。

## 【 0 0 8 7 】

図 1 3 は、プロキシCN機能群の配備方法の第 1 の実施形態を示した図である。

## 【 0 0 8 8 】

プロキシCNの機能群の配備方法として、HAからCNに送付される結合更新メッセージを、プロキシCNにて認識し、メッセージの実際の処理をプロキシCNにてCNに代わって行う。

## 【 0 0 8 9 】

本配備方法では、CMF、TCF、MHF、MAF、CDの全ての機能エンティティをCNの隣接ルータ（プロキシCN：CNが通常アクセスするデフォルトルータとして設定されている）に収容しているため、実装する場合には、本機能間の連携のための独自の外部インターフェースを必要としない。CNへ送付される結合更新メッセージは、デフォルトルータを兼ねるプロキシCNを経由するが、プロキシCN機能群の中のMHF（Message Handling Function）は、全てのパケットのヘッダ情報を検索する機能を持ち、Mobile IP制御メッセージを監視する。

## 【 0 0 9 0 】

検出された結合更新メッセージは、プロキシCNのCMF（Cache Management Function）に渡され、該CNのキャッシュデータ（CD）に反映される。

## 【 0 0 9 1 】

Mobile IP制御メッセージの検出は、IPヘッダの「Protocol」フィールドを参照し、（1）TCP（Transmission Control Protocol）もしくはUDP（Use

r Datagram Protocol) のいずれかに該当する、(2) TCP/UDPヘッダ中の「ポート番号」フィールドを参照し、これがMobile IP制御メッセージである、の二点を満たすパケットを「Mobile IP制御メッセージ」と判定する。該当しないものはデータパケットである。次に、前項を満たすパケットの中から、経路最適化のための結合キャッシュ管理メッセージかどうかを判定する。具体的には、Mobile IPヘッダの「Type」フィールドを参照する(e.g. Type: 結合更新メッセージ)。結合キャッシュ管理メッセージと判定されると、プロキシCNは、このメッセージの(本来の)宛先であるCNをIPヘッダのDestinationフィールドから特定する。前項にて特定されたCNを特定する情報をキーに、プロキシCNは該CNの結合キャッシュエントリを操作(結合キャッシュ更新)する。

## 【0092】

図14は、プロキシCN機能群の配備方法の第2の実施形態を示す図である。

## 【0093】

プロキシCN機能群の配備方法として、プロキシCNにおける結合更新メッセージの検出処理による負荷が大きい場合、HAにMHFの機能の一部を配備し、予め結合更新の送信元のHAにて結合更新メッセージの宛先を、デフォルトのCNから、プロキシCN宛に書き換える機能を配備する。

## 【0094】

すなわち、初回の結合更新メッセージは、HAはそのままプロキシCNに転送する。プロキシCNでは、本来CNに宛てて送信されてきた初回の結合更新メッセージを終端して、結合キャッシュの更新を行う。次に、プロキシCNは、HAに向けて、結合更新応答メッセージを送信する。そして、このメッセージにおいて、同じMNが移動したことにより送信されてきた結合更新メッセージについては、宛先をプロキシCNに書き換えて転送するようにHAに依頼する。HAは、これに従って、2回目以降の結合更新メッセージをプロキシCNに宛てて送信する。

## 【0095】

このようにすることにより、プロキシCNは、2回目以降の結合更新メッセージについては、メッセージの検出処理を行う必要がないので、プロキシCNの負

荷が軽減される。

【0096】

図15は、プロキシCN機能群の配備方法の第3の実施形態を示した図である。

【0097】

プロキシCN機能群の配備方法として、MHFをCNに配備し、MHFを含むその他の機能をプロキシCN内に配備する。結合更新メッセージは、本出願人の前出の先願同様、一旦CNまで送達される。ここで、CNには結合更新メッセージを検出し、これを登録先のプロキシCNへ転送する機能を持つ。

【0098】

これにより、やはり、結合更新メッセージだけがCNからプロキシCNに送られてくるので、プロキシCNが自身を通過する全てのメッセージを調べて、更新結合メッセージか否かを判断する処理が必要なくなり、やはり、プロキシCN自身のメッセージを処理する負荷が軽減される。

【0099】

Mobile IPメッセージ以外のデータパケットについては、CNから送信されたパケットを、デフォルトルータを兼ねるプロキシCNにて受信し、CNに装備される動作を代行する。すなわち、該パケットの発信元のCNが経路最適化を適用可能か否かを判定し、適用すべき端末で有ればプロキシCNのCMFにて該CNに対応したサービス制御を行い、TCFにてトンネリングパケットを生成し、送信する。

CNのプロキシCNへの登録手順について以下にまとめる。

・ Mobile IPを利用可能なCNの登録

(1) プロキシCNは、所属するネットワーク内にMobile IPのエージェント広告を発行（ブロードキャスト）する。

(2) Mobile IP機能を装備したCNは、前述のプロキシCNの広告を受信し、Mobile IPメッセージの登録要求（Registration Request）を該プロキシCNに対して送信する。

(3) プロキシCNは、AAAサーバによる認証にて、該CNの正当性を確認す



る。

(4) 認証完了後、プロキシCNは、該CNに関するキャッシュデータ（結合キャッシュ、サービスプロファイル）のエントリを生成する。

(5) プロキシCN内の登録処理が正常終了した場合、Mobile IPのRegistration Replyメッセージにて該CNに登録応答が返される。

・ Mobile IPを使用しないCNの登録

(1) Mobile IPを使用しないCNは、ダイヤルアップPPP (Point-to-Point Protocol) にてISP (Internet Service Provider) に接続を試みる。

(2) 該CNからの接続要求を受信したダイヤルアップサーバは、該CNの正当性を認証するために、ダイヤルアップサーバと関連した認証サーバに認証を依頼する。PPP接続の場合の認証方法ではPAP (Password Authentication Protocol)、CHAP (Challenge-Handshake Authentication Protocol) が使用される。

(3) 認証依頼を受けた認証サーバは、該CNの正当性が確認されると、該CNに関するサービスプロファイルを収容したサービスプロファイルデータベース（サービスプロファイルDB）から、該CNに関するサービスプロファイルを読み出す。

(4) 認証サーバは、該CNの登録要求先のプロキシCNに、前項で取得した、該CNのサービスプロファイルを送付する。

(5) (4) の通知に基づいて、プロキシCNは、該CNに関連する訪問者リストのエントリを生成すると共に、このエントリと経路最適化に関連する結合キャッシュ、及び、認証サーバから通知されたサービスプロファイルを保持するエントリを生成する。

(6) 認証サーバは、登録要求のあったCNに対して登録応答を返す。

【 0 1 0 0 】

CNの在圏確認について以下にまとめる。

・ Mobile IPを利用可能なCNの在圏確認

(1) 移動CNはMobile IPの機能として、登録時にプロキシCNとの間で合意された登録の有効期間 (Lifetime) より小さい周期にて再登録を繰り返す必要が

あり、Mobile IPの登録要求 (Registration Request) メッセージを現在登録先のプロキシCNに対して送出する。

(2) プロキシCNは、前述の再登録の要求を受信した場合は、該CNが在圏すると判定する。

(3) (2) に対して、登録の有効期間を経過してもプロキシCNが、該CNからの再登録を受信しない場合、Mobile IPの手順によって、該CNの登録を抹消する。具体的には、Mobile IPの機能の範囲内では該CNに関する訪問者リストエントリが削除されるが、同時に、この訪問者リストエントリと関連付けられた結合キャッシュ、サービスプロファイルも削除される。すなわち、Mobile IPの登録削除の手順と連動してプロキシCN機能に関連するデータも削除される。

・ Mobile IPを利用不可能なCNの在圏確認

方法 1

(1) プロキシCNは、該CNから発信されるパケットのフローを監視する。プロキシCNは個々のCNについて、訪問者リストエントリの一部を使用し、CNの在圏状態を記録する。登録中にCNがパケットを送信している状態では「在圏」となっている。

(2) 上記の監視において、一定期間、該CNが発信するパケットのフローが検出されない場合に、プロキシCNは、該CNが圏外へ移動した可能性を予想し、該CNの在圏状態を「保留」状態とする。

(3) 上記保留状態に於いて、更に一定期間、該CNからのパケット送出が検出されない場合、プロキシCNは、該CNが圏外へ移動したと判断する。

(4) ただし、上記(3)のパケット監視期間において、パケットを検出した場合には、再び「在圏」状態に戻る。

【 0 1 0 1 】

方法 2

(1) プロキシCN内で動作する周期監視タスクは、管理下にある全CNについて前回のパケット送出確認時刻 (確認タイムスタンプ) を検索する。

(2) 周期監視タスクは、個々のCNについて、確認タイムスタンプと現在時刻との差分を得る。この差分時刻がプロキシCN内の規定値よりも大きい場合、該

CNは一定期間以上パケット送出を行っていないと判断し、登録削除される。

(3) これに対して、差分時刻が規定値以内であれば、該CNは在圏すると判定し、パケット検出を行い、この結果パケットが検出されれば、確認タイムスタンプを最新のパケット検出時刻で更新する。パケットが検出されなければ、更新しない。

(4) 以上(1)～(4)をプロキシCNシステムが規定する周期にて繰り返し監視することで、周期的な在圏確認が可能となる。

・ Mobile IPを利用不可能な場合のリンクレイヤの回線切断

(1) CNは電話回線等でPPPによりアクセスサーバに接続中とする。

(2) CNは通信の終了にともない、リンクレイヤの回線切断メッセージがアクセスサーバに送信される。

(3) 回線切断メッセージを検出したアクセスサーバは、プロキシCN機能群のMHFに対し、該CNの回線切断を通知する。

(4) プロキシCN機能群のMHFは、MAFに対し、該CNが圏外に移動した旨のメッセージを送信する。

(5) MAFは、該CNに関する訪問者リストエントリを削除すると共に、CMFに対して、該CNに関する結合キャッシュ、サービスプロファイルの削除を依頼し、該CNの登録削除が完了する。

#### 【 0 1 0 2 】

図16及び図17は、図13の実施形態におけるIPサービス制御メッセージ処理を説明するフローチャートであり、図16は、CNがプロキシCNへの登録完了時点でキャッシュエリアが生成されている場合を示し、図17は、CNに最初の結合更新メッセージがプロキシCNに到達した時点でキャッシュエリアが生成される場合を示している。

#### 【 0 1 0 3 】

まず、図16においては、結合更新メッセージに付加された「サービスプロファイル」の対象となる端末(CN)のキャッシュが存在した場合は、単にキャッシュの更新のみを実行するが、何らかの原因(リソース不足等)でキャッシュエリアが存在しない場合は、異常シーケンスを採る。この場合、プロキシCNは受

信したキャッシュが正常に処理されなかったことを、送信元のHAに通知することができる。この通知は、Mobile IP拡張プロトコル（経路最適化）が定義する「結合応答（Binding Acknowledge）」メッセージを利用する。

#### 【0104】

よって、キャッシュ生成不能の場合、結合応答メッセージを生成し、受信先のプロキシCNにて正常処理されなかった旨の理由を示す値を格納し、HAに対して送信する。

#### 【0105】

図16において、まず、HAは、経路最適化の対象となるCNに対して結合更新メッセージ（プロファイルキャッシュを含む）を送信する。そして、この結合更新メッセージは、宛先のCNに対するデフォルトルータを兼ねるプロキシCNに到達する。プロキシCNでは、ステップS30でのパケット待ち状態を経て、ステップS31で、パケットを受信検出し、受信する全てのパケットの（データ、Mobile IP制御メッセージに無関係に）ヘッダ部を検索し、CN宛の結合更新メッセージか否かを判定する（ステップS32）。結合更新メッセージであるか否かの判断の方法としては、IPヘッダの「Protocol」フィールドを参照し、（1）TCPもしくはUDPのいずれかに該当する、（2）TCP/UDPヘッダ中の「ポート番号」フィールドを参照し、これがMobile IP制御メッセージである、の二点を満たすパケットを「Mobile IP制御メッセージ」と判定する。受信したパケットがデータパケットである場合には、ステップS33で、その他のパケット処理を行って、ステップS30に戻る。

#### 【0106】

ステップS32において、結合更新メッセージであると判断された場合には、結合更新メッセージのパケットの中から、経路最適化の結合キャッシュ管理メッセージかどうかを判定する。具体的には、Mobile IPヘッダの「Type」フィールドを参照する（e.g.Type：結合更新メッセージ）。結合キャッシュ管理メッセージと判定されると、プロキシCNは、このメッセージの（本来の）宛先であるCNをIPヘッダのDestinationフィールドから特定する。そして、結合更新メッセージと判定されたパケットについては、ステップS34において、宛先CNに

該当するキャッシュが存在するか否かが判断され、該当するキャッシュが存在する場合には、プロキシCN機能群により、プロキシCNに保持される結合キャッシュ、及び、サービスプロファイルキャッシュに蓄積、操作され、本来の宛先のCNに要求される動作、機能を代行する。ステップS 3 4において、該当するキャッシュがない場合には、ステップS 3 6において、サービス制御対象外の結合応答メッセージを生成し、ステップS 3 7において、結合応答メッセージを送出して、ステップS 3 0に戻る。

## 【 0 1 0 7 】

図 1 7 においては、プロキシCNにおけるCNからの最初の結合更新メッセージがプロキシCNに到達した時点でキャッシュエリアが生成される場合の packets 処理のフローを示している。

## 【 0 1 0 8 】

この場合は、「該当キャッシュが無い場合の処理」が異なり、当該CNに関する「最初の」結合更新メッセージ（+サービスプロファイルキャッシュ）を受信した場合、新規にキャッシュエリアを作成し、サービスプロファイルキャッシュのデータを格納する。

## 【 0 1 0 9 】

まず、ステップS 4 0において、パケット待ち状態となり、ステップS 4 1で、パケット受信検出を行い、ステップS 4 2において、受信したパケットが結合更新メッセージであるか否かを判断する。結合更新メッセージでないと判断された場合には、ステップS 4 3において、その他のパケット処理を行い、結合更新メッセージであると判断された場合には、ステップS 4 4に進む。

## 【 0 1 1 0 】

ステップS 4 4では、メッセージの宛先であるCNに該当する結合キャッシュ（あるいは、単に、キャッシュ）があるか否かを判断し、結合キャッシュが存在する場合には、ステップS 4 5においてキャッシュを更新し、該当するキャッシュが存在しない場合には、ステップS 4 6において、キャッシュを生成して、ステップS 4 0に戻る。

## 【 0 1 1 1 】

図 1 8 ～ 2 1 は、図 1 4 の実施形態における I P サービス制御メッセージ処理を示すフローチャートであり、図 1 8 は、C N がプロキシ C N への登録完了時点でキャッシュエリアが生成される場合であり、図 1 9 は、C N に最初の結合更新メッセージがプロキシ C N に到達した時点でキャッシュエリアが生成される場合であり、図 2 0 は、各機能エンティティの packets 処理概要であり、H A の受信処理判定を示し、図 2 1 は、各機能エンティティの packets 処理概要であり、H A の送信処理判定を示す図である。

#### 【 0 1 1 2 】

まず、H A は C N を宛先として「最初の」結合更新メッセージを送信する。プロキシ C N は、ステップ S 5 0 において、packets 待ちとなっており、ステップ S 5 1 で packets 受信検出を行う。そして、ステップ S 5 2 において、受信した packets が結合更新メッセージであるか否かを判断し、結合更新メッセージでない場合には、ステップ S 5 3 において、その他の packets 処理を行って捨て S 5 0 に戻る。ステップ S 5 2 において、結合更新メッセージであると判断された場合には、C N のデフォルトルータであるプロキシ C N は、結合更新メッセージの宛先を調べ、宛先がプロキシ C N であった場合には、ステップ S 5 8 において、対象キャッシュが存在するか否かを判断し、対象キャッシュが存在する場合には、ステップ S 5 9 において、キャッシュを更新し、対象キャッシュが存在しない場合には、ステップ S 6 0 において、結合応答メッセージを生成し、ステップ S 6 1 において、結合応答メッセージを送出し、ステップ S 5 0 に戻る。

#### 【 0 1 1 3 】

ステップ S 5 4 において、結合更新メッセージの宛先が C N である場合には、この結合更新メッセージを、同メッセージを本来の宛先である C N には送達せずに、同メッセージに含まれる結合キャッシュ、及び、サービスプロファイルキャッシュを生成し、保持する（ステップ S 5 5）。そして、プロキシ C N の M H F 部は、独自メッセージとして「結合更新応答メッセージ」を、結合更新メッセージの送信元の H A に対して返信する（ステップ S 5 6、S 5 7）。このメッセージは、該プロキシ C N が C N の代理として以後に送信される結合更新メッセージを処理することを宣言するものである。

## 【0114】

また、デフォルトルータにプロキシCN機能が無ければ、結合更新はCNに送達され、CN自身が結合更新を処理する。

## 【0115】

「結合更新応答メッセージ」を受信したHAは、送信元のプロキシCNとこの配下にある本来の宛先であるCNの情報を関連付け、以後（二回目以降）に該CNに送達される結合更新メッセージの宛先を該プロキシCNに変更して送信する。したがって、該CNに関連する二回目以降の結合更新メッセージは、プロキシCNが受信し、処理する。

## 【0116】

図19は、CNに最初の結合更新メッセージがプロキシCNに到達した時点でキャッシュエリアが生成される場合のプロキシCNの処理を示している。

## 【0117】

まず、ステップS70において、パケット待ち状態となり、ステップS71において、パケットを受信検出する。ステップS72において、受信したパケットが結合更新メッセージであるか否かを判断し、ステップS73において、その他のパケット処理を行い、ステップS70に戻る。

## 【0118】

ステップS72において、受信したパケットが結合更新メッセージであると判断された場合には、ステップS74において、結合更新メッセージの宛先を調べ、宛先がプロキシCNであった場合には、ステップS78において、更新対象のキャッシュが存在するか否かを判断し、存在する場合には、ステップS79において、キャッシュを更新し、存在しない場合には、ステップS80において、キャッシュを生成する。

## 【0119】

ステップS74において、結合更新メッセージの宛先がCNの場合には、ステップS75において、キャッシュエリアを生成し、結合更新応答メッセージを生成して、HA宛てに結合更新応答メッセージを送出する（ステップS76、S77）。

## 【 0 1 2 0 】

図 2 0 は、図 1 4 の実施形態における各機能エンティティの packets 処理の概要であり、H A の受信処理判定を示すフローチャートである。

## 【 0 1 2 1 】

H A は、ステップ S 8 5 において、packets 受信待ち状態となっている。packets が送信されてくると、ステップ S 8 6 において、packets 受信検出を行い、ステップ S 8 7 において、受信した packets が結合更新応答メッセージであるかを判断する。受信した packets が結合更新応答メッセージでない場合には、ステップ S 8 5 に戻って、次の packets が送信されてくるのを待つ。ステップ S 8 7 において、受信した packets が結合更新応答メッセージであると判断された場合には、ステップ S 8 8 において、該当する C N に関する情報エントリの内、結合更新の宛先を変更する。そして、ステップ S 8 5 に戻って、他の packets の受信待ち状態となる。

## 【 0 1 2 2 】

図 2 1 は、図 1 4 の実施形態における各機能エンティティの packets 処理の概要であり、H A の送信処理判定を示すフローチャートである。

## 【 0 1 2 3 】

まず、ステップ S 9 0 において、H A が、packets 送信準備を完了すると、ステップ S 9 1 において、packets 種別を分析し、ステップ S 9 2 において、受信した packets が結合更新メッセージであるかを判断する。結合更新メッセージでない場合には、ステップ S 9 6 に進んで、packets 送信処理（packets の宛先に向けた送信処理）を行って、ステップ S 9 0 に戻る。ステップ S 9 2 において、受信した packets が結合更新メッセージであると判明した場合には、送信 packets の宛先が結合更新応答により、変更されているかを検索し（ステップ S 9 3 ）、結合更新メッセージの宛先変更が必要かをステップ S 9 4 において行う。ステップ S 9 4 において、宛先変更が必要でないと判断された場合には、ステップ S 9 6 において、受信した packets の宛先に向けて packets を送信する。ステップ S 9 4 において、宛先変更が必要と判断された場合には、ステップ S 9 5 において、packets の宛先を変更し、ステップ S 9 6 で、packets を変更され



た宛先（プロキシCN）に向けて送信する。パケット送信処理が終わると、ステップS90に戻り、処理を繰り返す。

#### 【0124】

図22～図24は、図15の実施形態におけるIPサービス制御メッセージ処理を示すフローチャートであり、図22は、CNがプロキシCNへの登録完了時点でキャッシュエリアが生成されている場合であり、図23は、当該CNに最初の結合更新メッセージがプロキシCNに到達した時点でキャッシュエリアが生成される場合であり、図24は、各機能エンティティのパケット処理概要の内、CNの判定処理を示すフローチャートである。

#### 【0125】

図22においては、まず、HAは、CNを宛先として結合更新メッセージを送信する。CNのデフォルトルータであるプロキシCNは、パケット待ち状態（ステップS100）において、この結合更新メッセージを受信するが（ステップS101）、受信したメッセージが結合更新メッセージであって、CNに転送すべきものか否かを判断して（ステップS102）、同メッセージを通常のルータと同様にCNに送付し、ステップS100に戻る。

#### 【0126】

ステップS102に於いて、結合更新転送メッセージ、すなわち、自身に向けて送られてきたものであると判断した場合には、ステップS103において、当該CNのキャッシュが存在するか否かの判断を行い、キャッシュが存在する場合には、ステップS104において、キャッシュエントリを更新し、ステップS100に戻る。ステップS103において、当該CNのキャッシュが存在すると判断した場合には、ステップS105において、結合応答メッセージを生成し、ステップS106において、

CNは、プロキシCNから転送されてきた、受信したパケットが、結合更新メッセージであることを検出する。結合更新メッセージを検出したCNは、ここで独自メッセージとして「結合更新転送メッセージ」を構成し、登録先のプロキシCNに対して送出する。同メッセージの内容は、ヘッダ情報としてプロキシCNが「結合更新メッセージ」と認識可能な情報を持ち、ペイロードとして、結合更

新メッセージに含まれる、結合キャッシュデータ、サービスプロファイルデータとなる。配下のCNが発信した「結合更新転送メッセージ」を受信したプロキシCNは、ヘッダ情報から結合更新転送メッセージであることを検出する。プロキシCNは、検出されたメッセージに含まれる該CNに関するデータを登録する。

## 【 0 1 2 7 】

図 2 3 は、CNに最初の結合更新メッセージがプロキシCNに到達した時点でキャッシュエリアが生成される場合のプロキシCNの処理を示すフローチャートである。

## 【 0 1 2 8 】

まず、ステップ S 1 1 0 において、プロキシCNは、パケット待ちの状態となっている。ステップ S 1 1 1 で、パケットを受信検出すると、ステップ S 1 1 2 で、受信したパケットが結合更新メッセージであり、CNに転送すべきものか否かを判断する。転送すべきものではない場合には、ステップ S 1 1 0 に戻って、処理を繰り返す。

## 【 0 1 2 9 】

ステップ S 1 1 2 において、受信したパケットが結合更新転送メッセージである、と判断した場合には、ステップ S 1 1 3 において、当該CNへの初回の結合更新転送メッセージであるか否かを判断する。初回の場合には、ステップ S 1 1 5 において、キャッシュエントリを生成してステップ S 1 1 0 に進み、ステップ S 1 1 3 において、初回でないと判断した場合には、ステップ S 1 1 4 において、キャッシュエントリを更新して、ステップ S 1 1 0 に戻る。

## 【 0 1 3 0 】

図 2 4 は、CNの判定処理を示すフローチャートである。

## 【 0 1 3 1 】

まず、ステップ S 1 2 0 において、パケット待ち状態となっている。ステップ S 1 2 1 で、パケットを受信すると、ステップ S 1 2 2 で、結合更新メッセージであるか否かを判断する。結合更新メッセージでない場合には、ステップ S 1 2 0 に戻って、パケット待ちとなる。ステップ S 1 2 2 において、受信したパケットが結合更新メッセージであると判断された場合には、ステップ S 1 2 3 におい

て、結合更新転送メッセージを生成し、ステップ S 1 2 4 において、プロキシ CN に対し、結合更新転送メッセージを送出し、ステップ S 1 2 0 に戻る。

【 0 1 3 2 】

以下には、結合更新メッセージではない、データパケットの処理に関する説明を行う。

(1) プロキシ CN 配下の CN が、特定の MN を宛先として、データパケットを送信する。

(2) 上記のデータパケットは、デフォルトルータを兼ねるプロキシ CN に到達する。

(3) プロキシ CN は、本データパケットの発信元を特定し、訪問者リストの中から該当するエントリを検索する。

(4) 発信元 CN の訪問者エントリから、該 CN が経路最適化の対象であることを判定する。

(5) 該 CN が発信するパケットが経路最適化の対象であると判断されると、プロキシ CN は、制御を T C F (Tunneling Capability Function) に渡し、トンネルパケットの生成を依頼する。

(6) T C F はトンネルパケットを生成し、プロキシ CN 内のルータ機能部に、このデータ及び制御権を渡し、送信を依頼する。

(7) プロキシ CN 内のルータ機能部は生成されたトンネルパケットを送出する。

【 0 1 3 3 】

以上、本発明を特定の実施形態に基づいて説明してきたが、本発明は、上記実施形態に限定されるものではなく、当業者によってなされる様々な変形も含むものである。

【 0 1 3 4 】

特に、前述の機能群 CMF、T C F、MHF、CD、MAF のそれぞれの配置は、上記実施形態に限定されるものではなく、CN の接続されるネットワーク側のいずれかの箇所に配置されれば十分である。

【 0 1 3 5 】

【発明の効果】

本発明によれば、対応端末（CN）に持たざるを得なかった機能群をネットワーク側に集約し、CNへの機能追加を不要（もしくは最小限の追加）にて同等機能を提供することが可能となる。

【0136】

従って、処理能力の低い携帯型端末等でも、機能追加、処理負荷増大の心配なく個別サービス制御を利用することが可能となる。

【0137】

更に、本発明によれば、ネットワーク側に集約された機能群を有する隣接ルータ（プロキシCN）への登録手段として、特定のプロトコルによる登録メカニズムを利用する手段の他に、該特定のプロトコルが使用できないリンクレイヤのCNの登録を受け付ける機能を用意し、リンクレイヤとの独立性を確保した。

【0138】

従って、多様なリンクレイヤにより、プロキシCNへの登録及び、個別サービス制御を利用することが可能となる。

【図面の簡単な説明】

【図1】

Mobile IPを説明する図である。

【図2】

図1の通信経路を抜き出した模式図である。

【図3】

本発明の一実施形態のネットワーク構成を示す図である。

【図4】

サービスプロファイルの例を示す図である。

【図5】

プロキシCNへのCNの登録処理を示す図である。

【図6】

CNがプロキシCNに登録されるまでの基本的な手順を示すシーケンス図である。

【図 7】

プロキシCN内の個別サービス制御データの管理方法を示す図である。

【図 8】

CNの在圏管理方法の一実施形態を示すシーケンス図（その 1）である。

【図 9】

CNの在圏管理方法の一実施形態を示すシーケンス図（その 2）である。

【図 1 0】

CNの在圏管理方法の別の実施形態を示した図（その 1）である。

【図 1 1】

CNの在圏管理方法の別の実施形態を示した図（その 2）である。

【図 1 2】

CNの在圏管理方法の別の実施形態を示した図（その 3）である。

【図 1 3】

プロキシCN機能群の配備方法の第 1 の実施形態を示した図である。

【図 1 4】

プロキシCN機能群の配備方法の第 2 の実施形態を示す図である。

【図 1 5】

プロキシCN機能群の配備方法の第 3 の実施形態を示した図である。

【図 1 6】

図 1 3 の実施形態における I P サービス制御メッセージ処理を説明するフローチャート（その 1）である。

【図 1 7】

図 1 3 の実施形態における I P サービス制御メッセージ処理を説明するフローチャート（その 2）である。

【図 1 8】

図 1 4 の実施形態における I P サービス制御メッセージ処理を示すフローチャート（その 1）である。

【図 1 9】

図 1 4 の実施形態における I P サービス制御メッセージ処理を示すフローチャ

ート（その２）である。

【図 2 0】

図 1 4 の実施形態における I P サービス制御メッセージ処理を示すフローチャート（その３）である。

【図 2 1】

図 1 4 の実施形態における I P サービス制御メッセージ処理を示すフローチャート（その４）である。

【図 2 2】

図 1 5 の実施形態における I P サービス制御メッセージ処理を示すフローチャート（その１）である。

【図 2 3】

図 1 5 の実施形態における I P サービス制御メッセージ処理を示すフローチャート（その２）である。

【図 2 4】

図 1 5 の実施形態における I P サービス制御メッセージ処理を示すフローチャート（その３）である。

【図 2 5】

従来技術のポリシー（Policy）によるネットワークにおける品質制御の例を示す図である。

【符号の説明】

- 1 0        F A (Foreign Agent)
- 1 1        H A (Home Agent)
- 1 2        M N (Mobile Node)
- 1 3        C N (Correspondent Node)
- 2 0        Mobile IPネットワーク
- 2 1        I P 転送網
- 2 2、2 7        サービスプロファイル D B
- 2 3        プロキシ C N 関連機能
- 2 4        プロキシ C N

特 2 0 0 0 - 0 3 2 3 7 2

2 5      C N

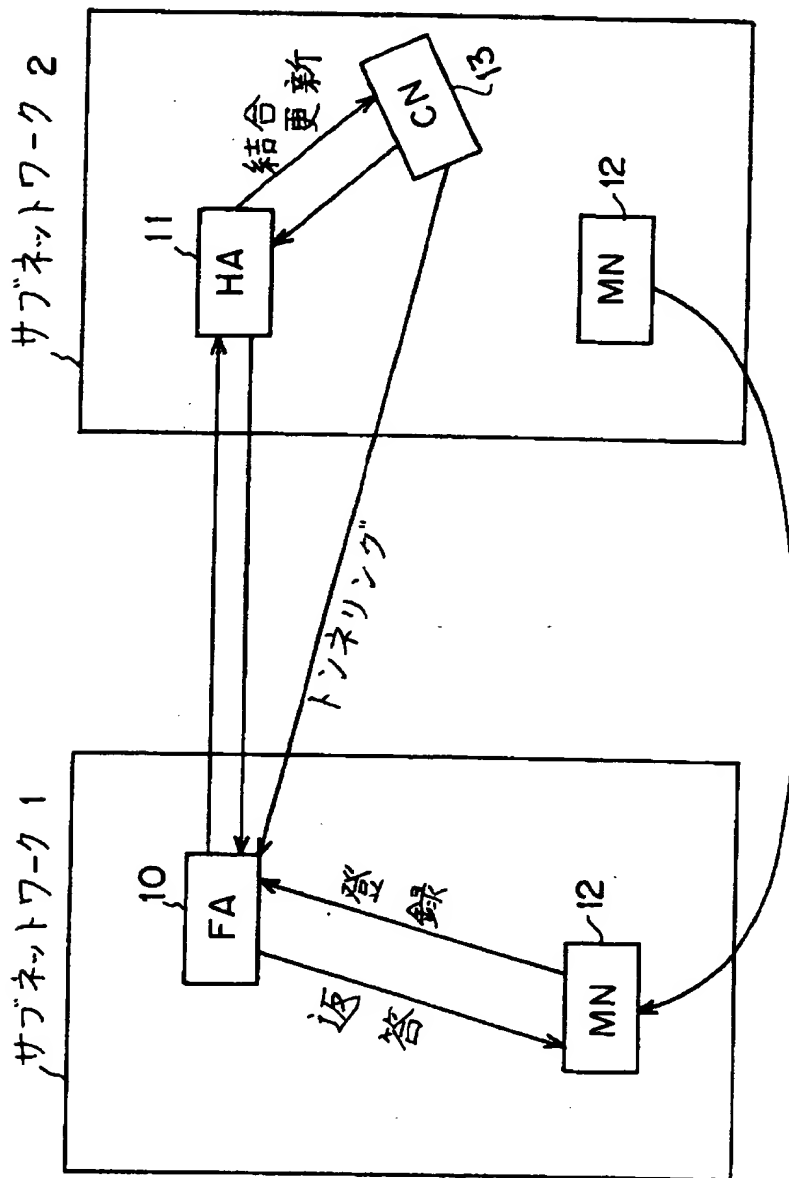
2 6      H A

【書類名】

図面

【図1】

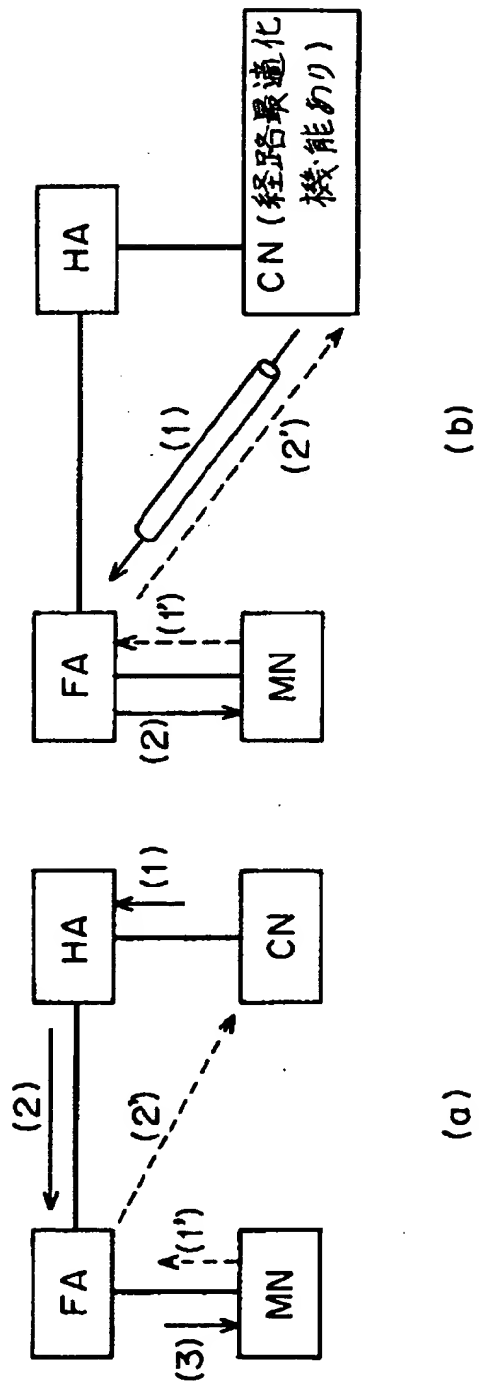
Mobile IP を説明する図





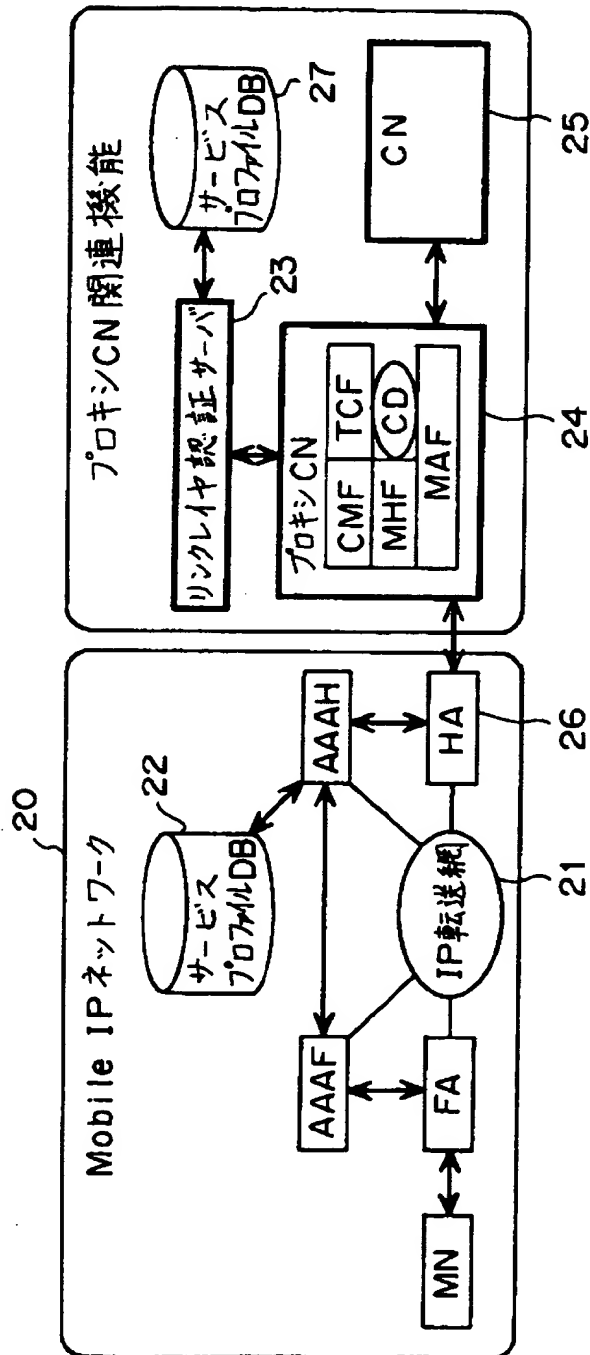
【図 2】

図 1 の通信経路を抜き出した模式図



【図 3】

本発明の一実施形態の  
ネットワーク構成を示す図



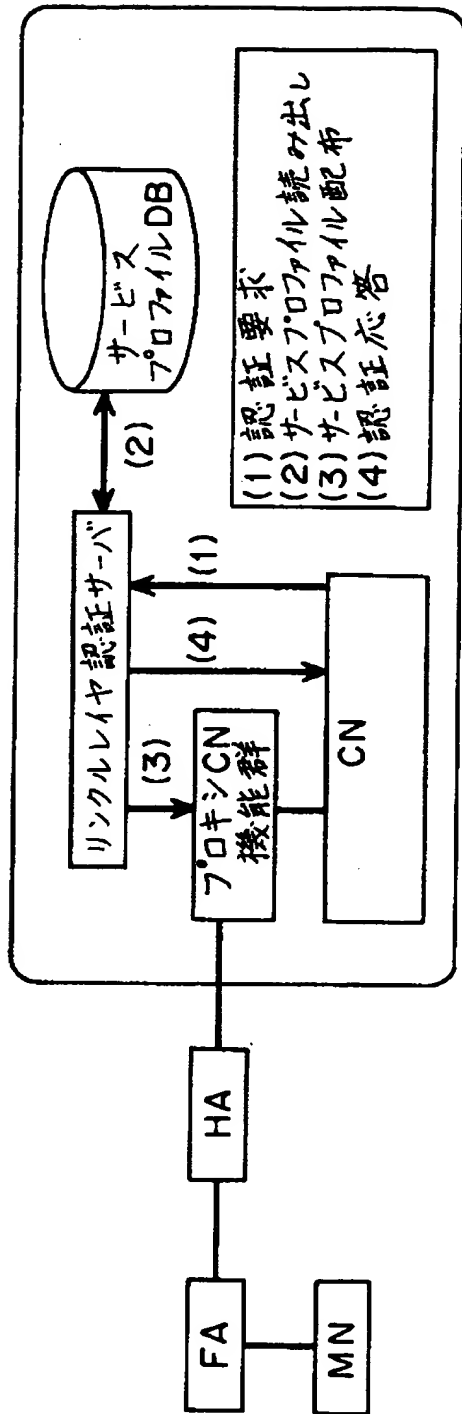
【図 4】

サービスプロファイルの例を示す図

構成情報	詳細構成情報	説明
制御対象パケット情報	送信元アドレス	移動ノードのホームアドレス等
	送信元ポート番号	IPヘッダ中のポート番号
	送信先アドレス	IPヘッダ中の受信先アドレス
	送信先ポート番号	IPヘッダ中の受信先ポート番号
	カプセル化(暗号化)手法	
ルーティング/パケット 編集情報	転送先アドレス	制御の結果の転送先アドレス
	IPbのTOS (Type Of Service) 値	サービス種別
	カプセル開放の指示	
	次サービス制御種別	Differentiated Services 等の IPトラヒック制御の適用等に関 する情報
個別制御情報		

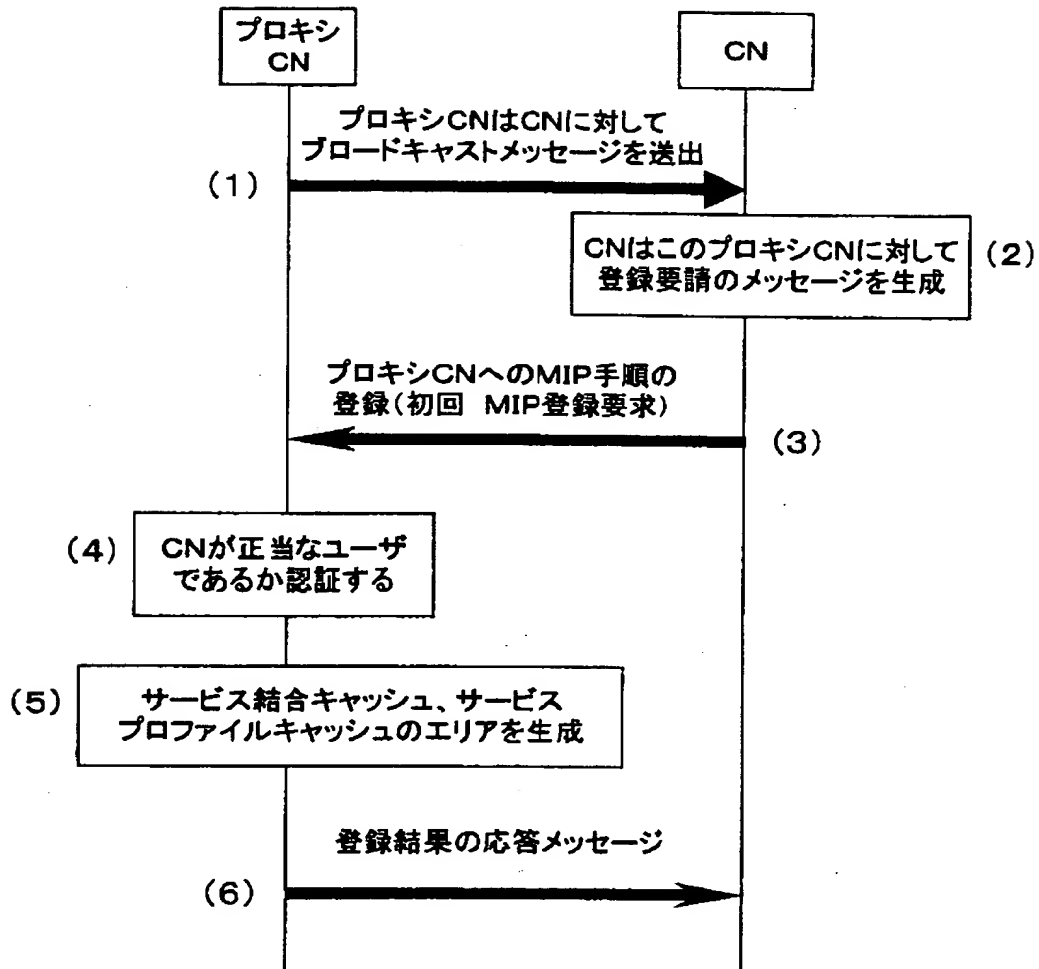
【図 5】

プロキシCNへのCNの登録処理を示す図



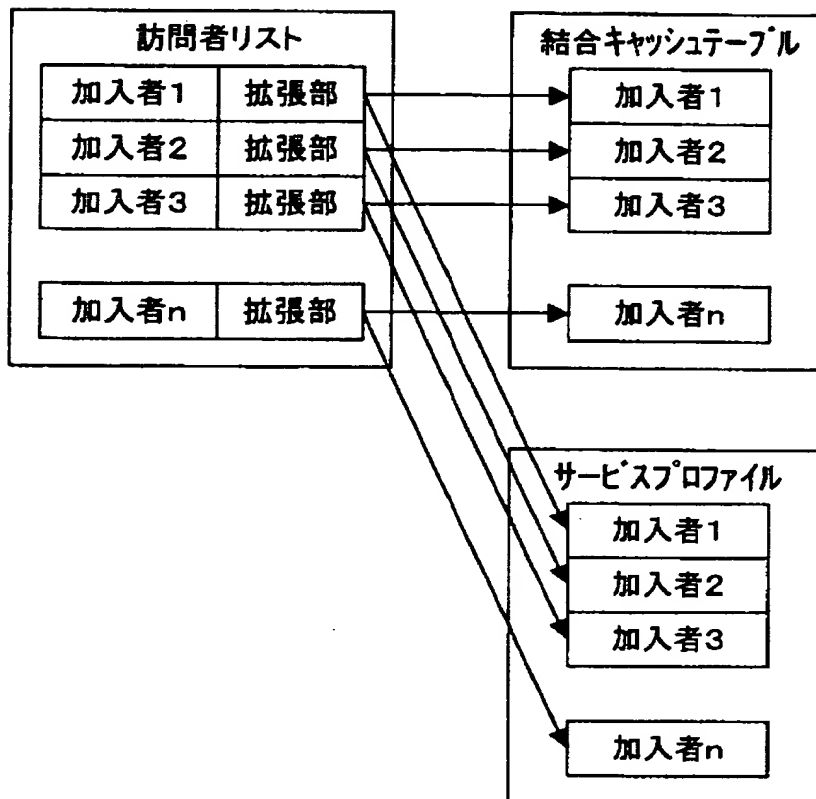
【図 6】

CNがプロキシCNに登録されるまでの基本的な手順を示すシーケンス図



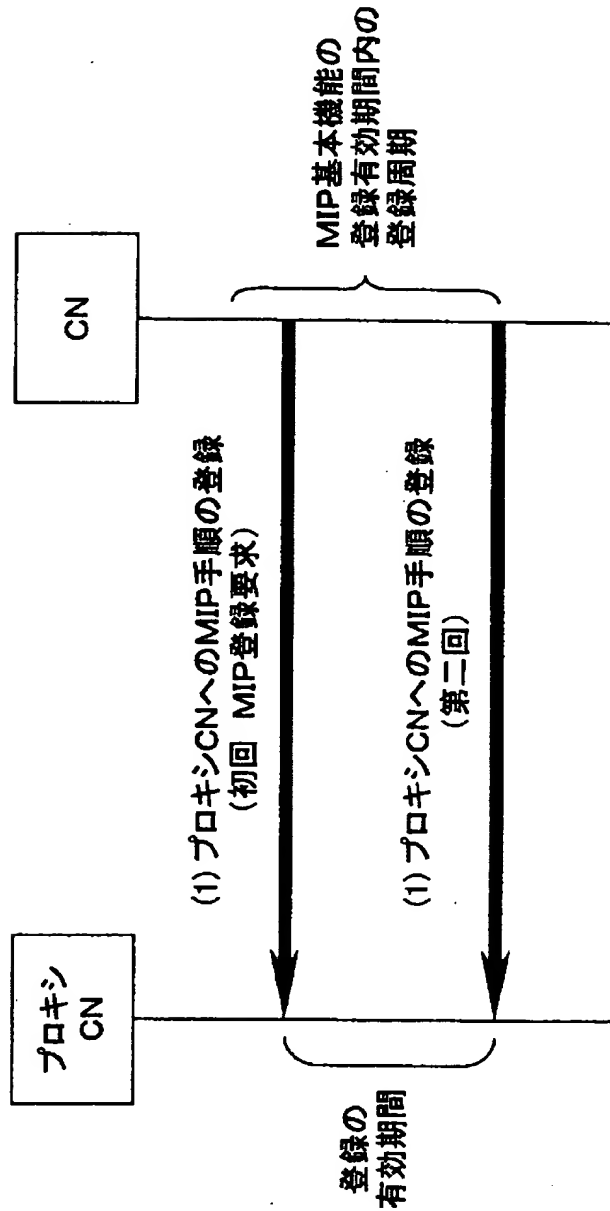
【図 7】

プロキシCN内の個別サービス制御データの  
管理方法を示す図



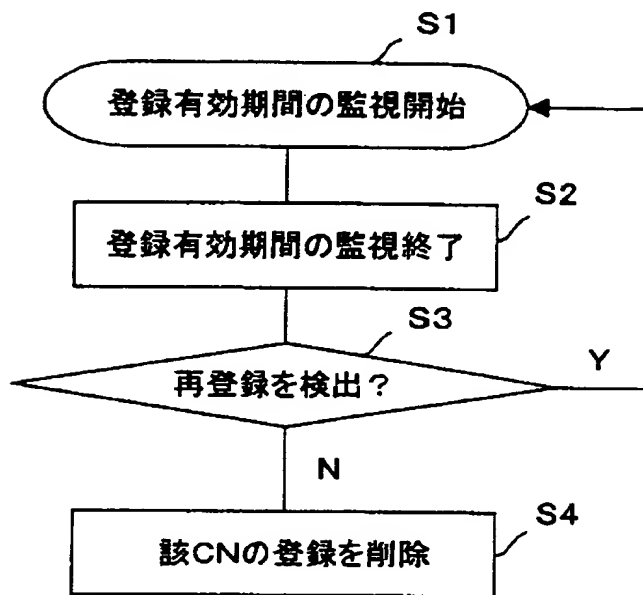
【図 8】

CNの在圏管理方法の  
一実施形態を示すシーケンス図(その1)



【図 9】

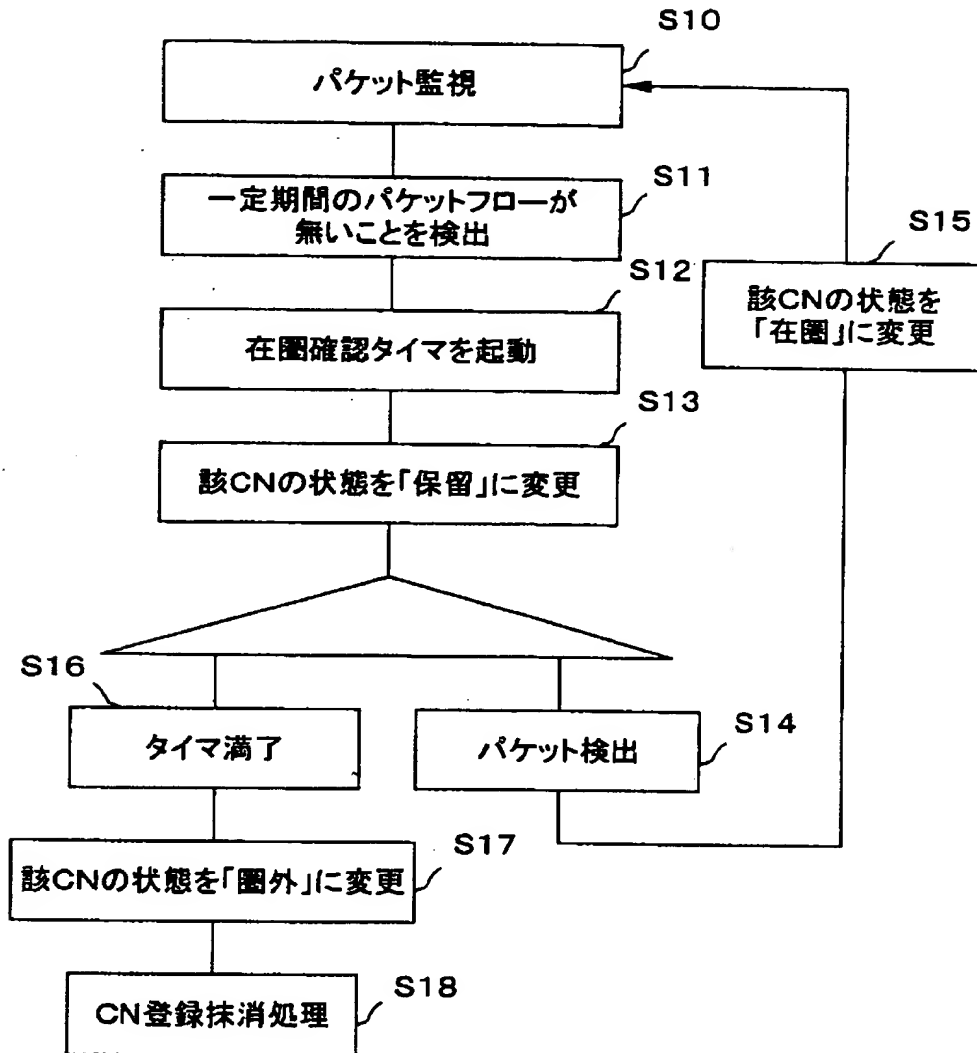
CNの在圏管理方法の  
一実施形態のを示すシーケンス図(その2)





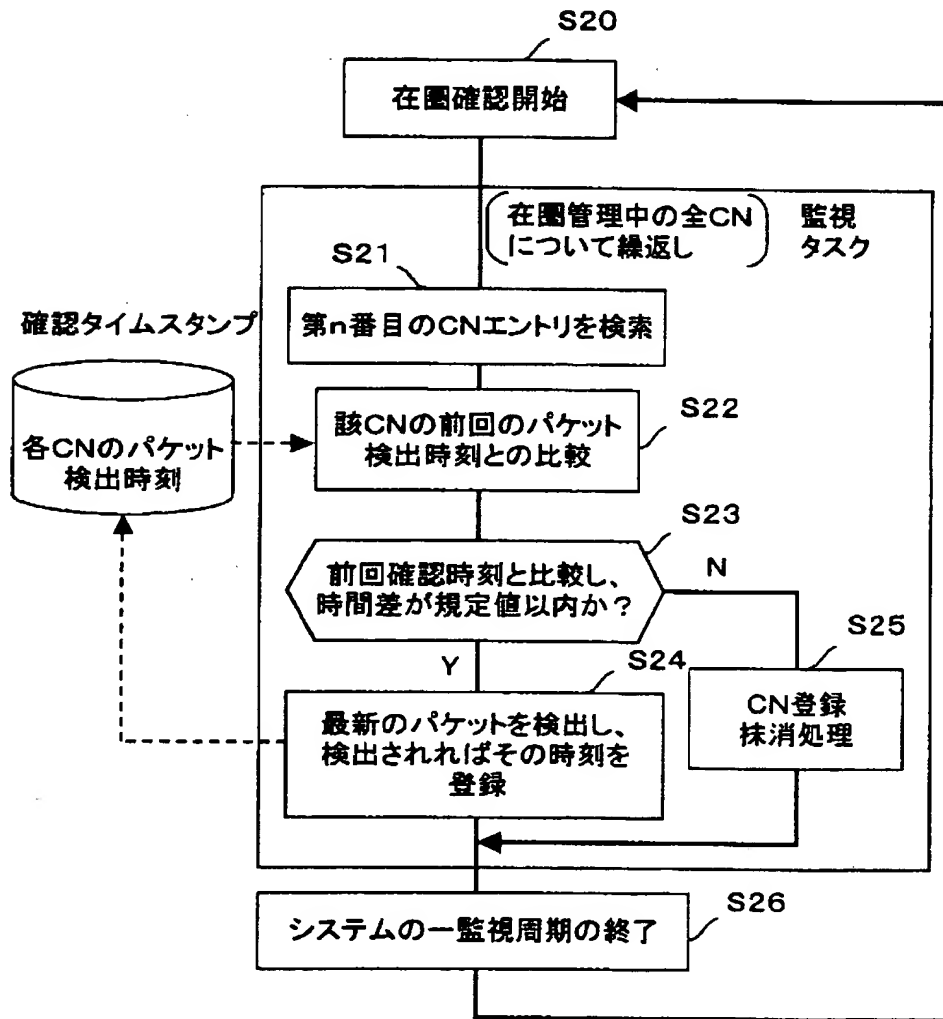
【図10】

CNの在圏管理方法の別の実施形態を示した図(その1)



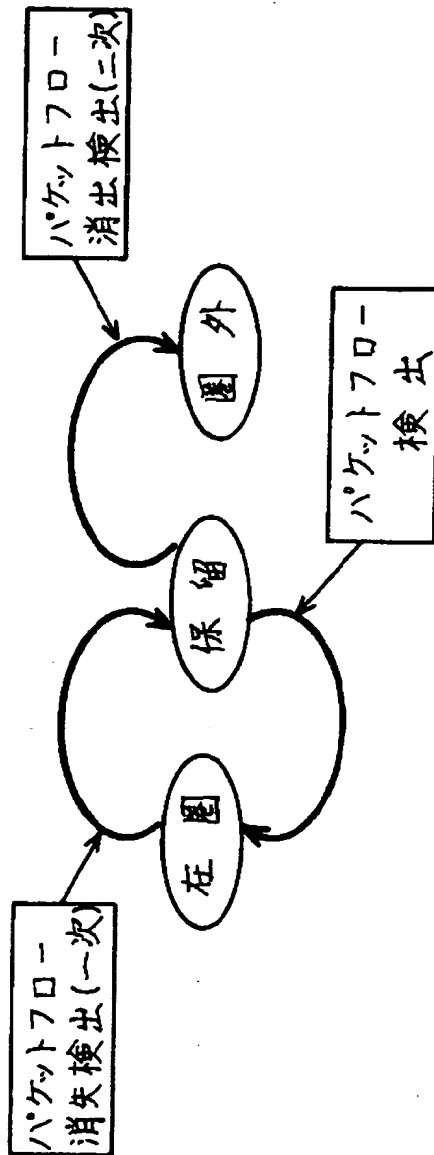
【図 11】

CNの在圏管理方法の別の実施形態を示した図(その2)



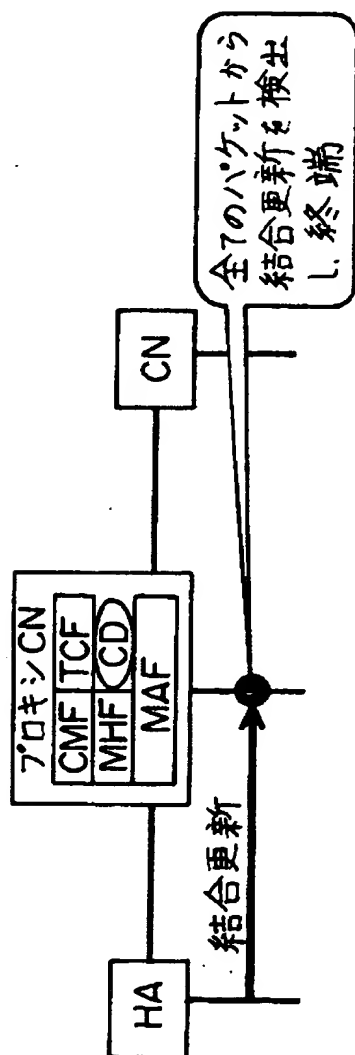
【図 1 2】

CNの在圏管理方法の別の  
実施形態を示した図 (その3)



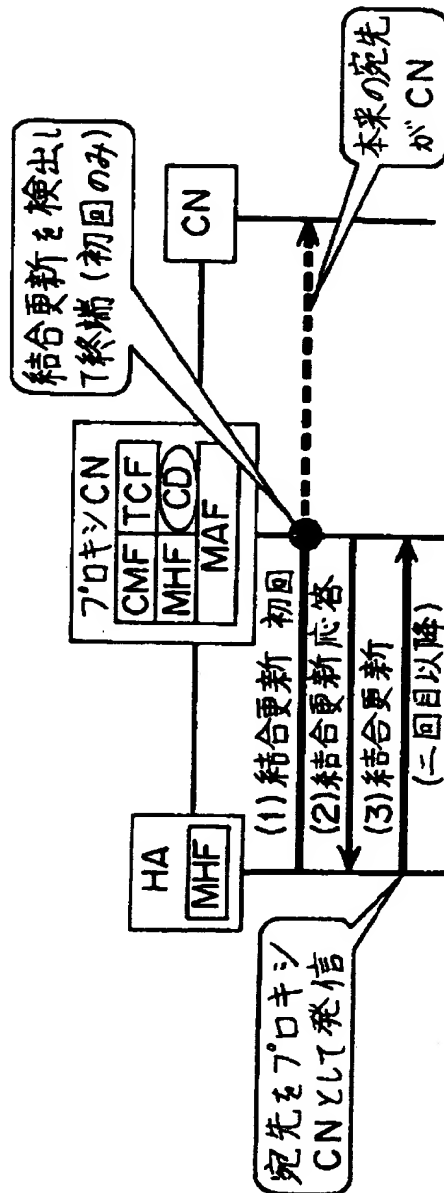
【図13】

プロキシCN機能群の  
配備方法の第1の実施形態を示した図



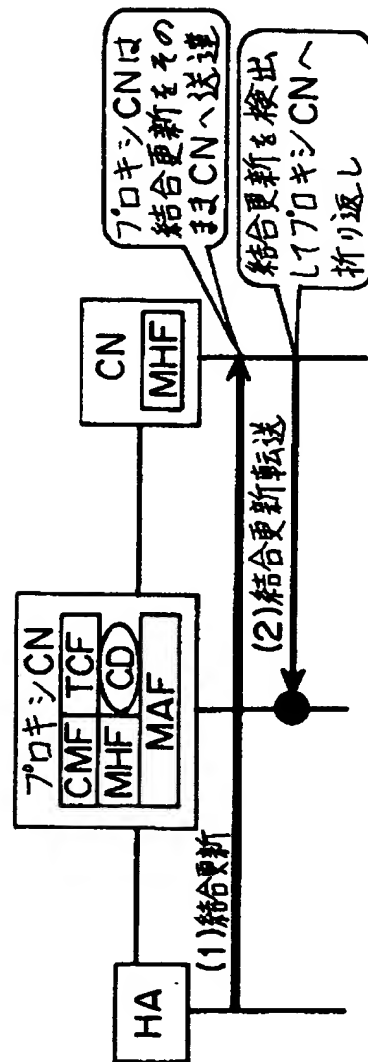
【図 1 4】

プロキシCN機能群の  
配備方法の第2の実施形態を示した図



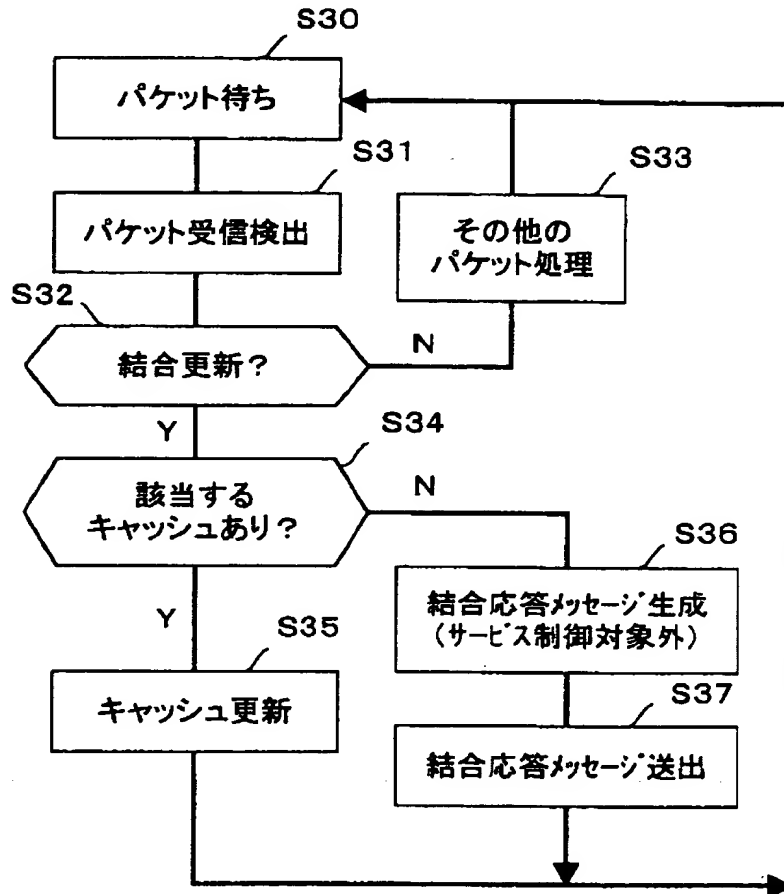
【図15】

プロキシCN機能群の  
配備方法の第3の実施形態を示した図



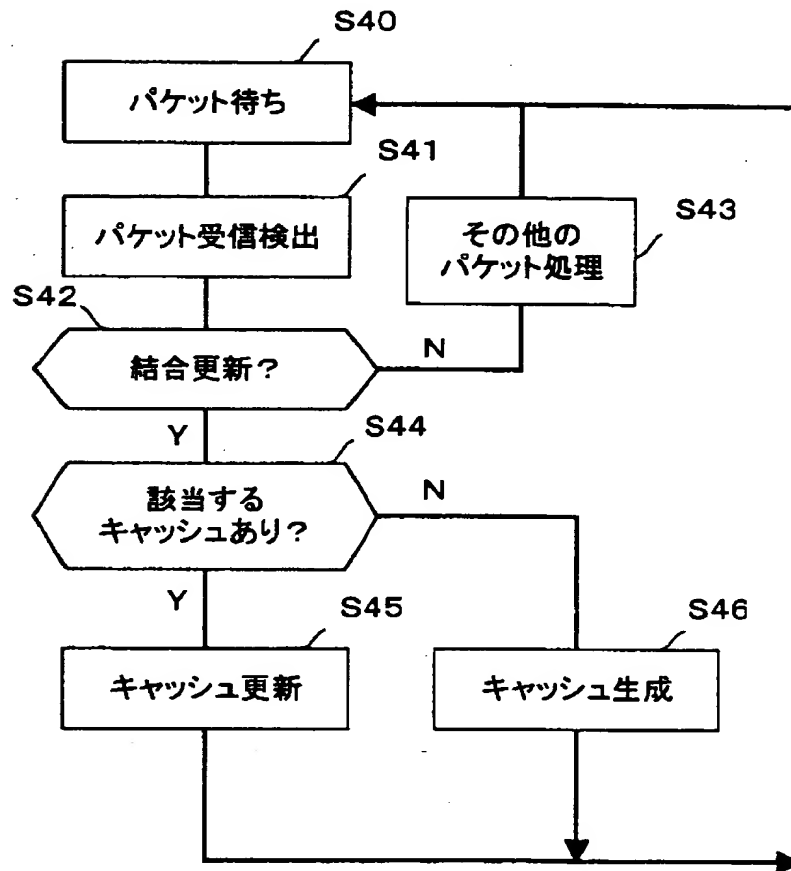
【図 16】

図13の実施形態におけるIPサービス制御  
メッセージ処理を説明するフローチャート(その1)



【図 1 7】

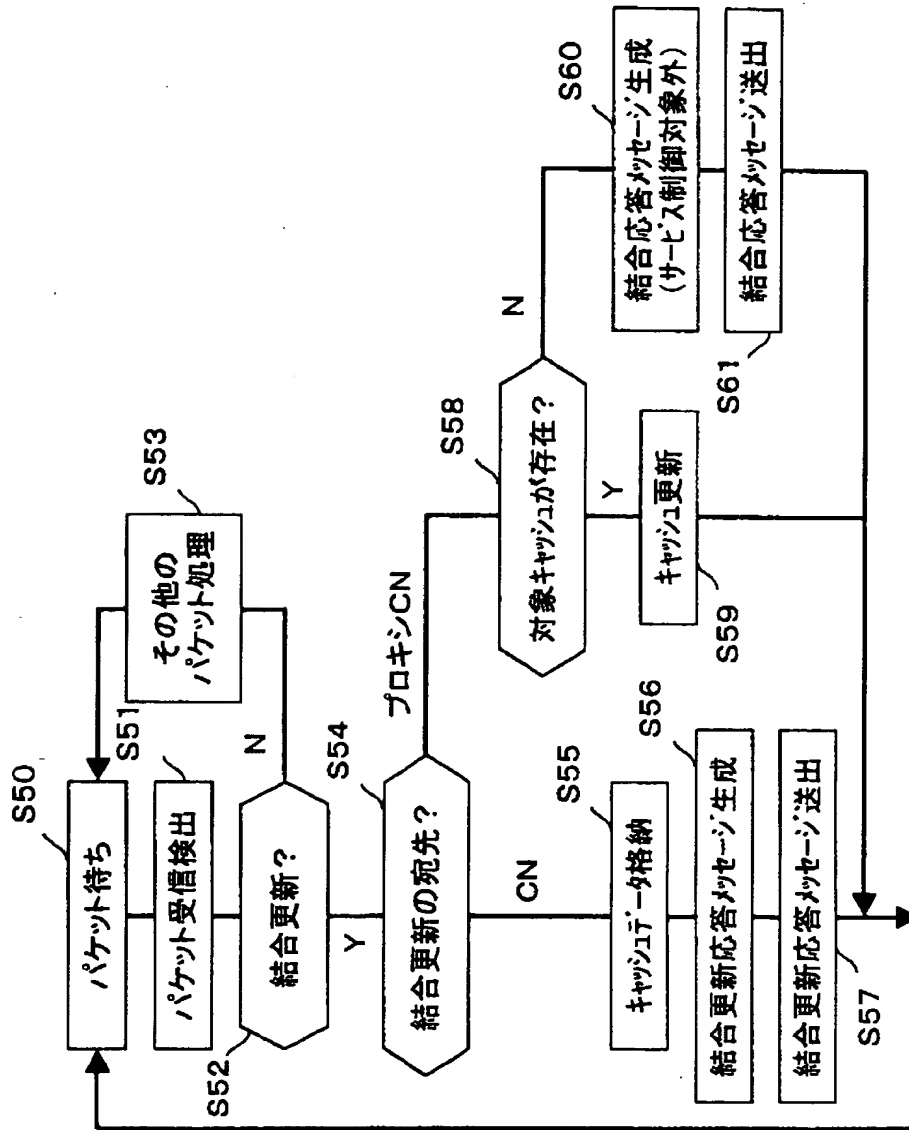
図13の実施形態におけるIPサービス制御  
メッセージ処理を説明するフローチャート(その2)





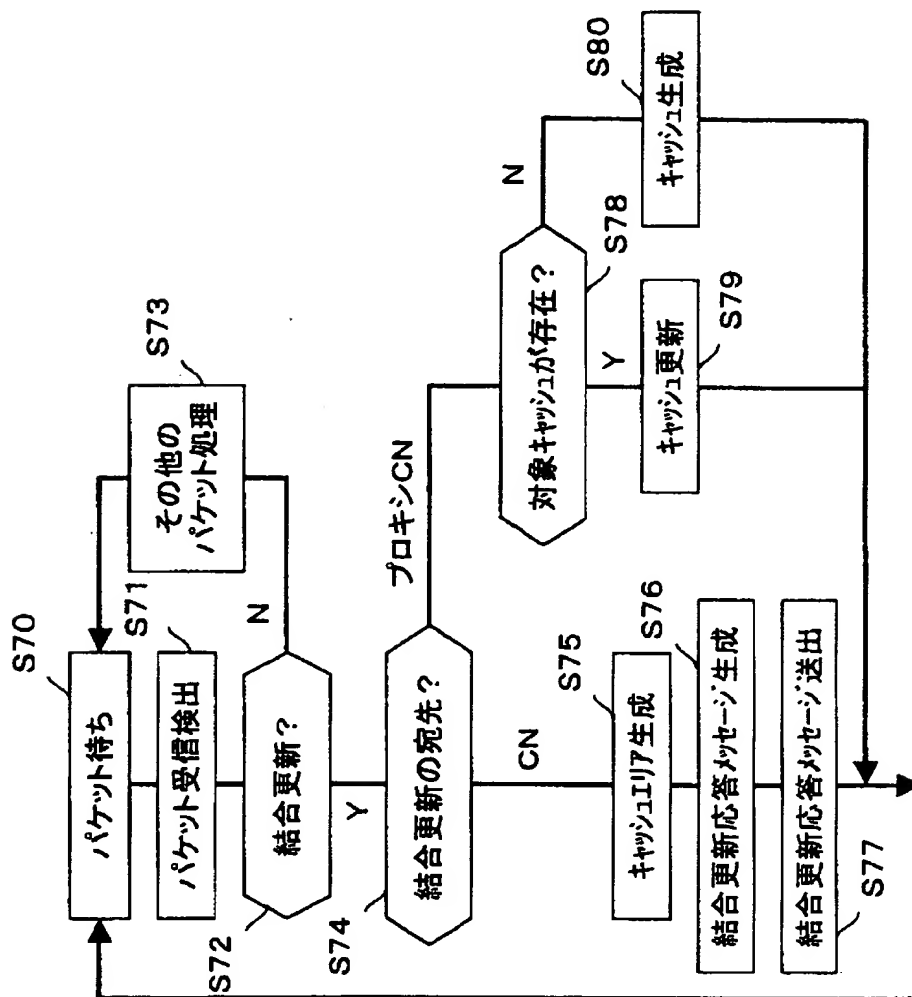
【図 1 8】

図14の実施形態におけるIPサービス制御  
メッセージ処理を示すフローチャート(その1)



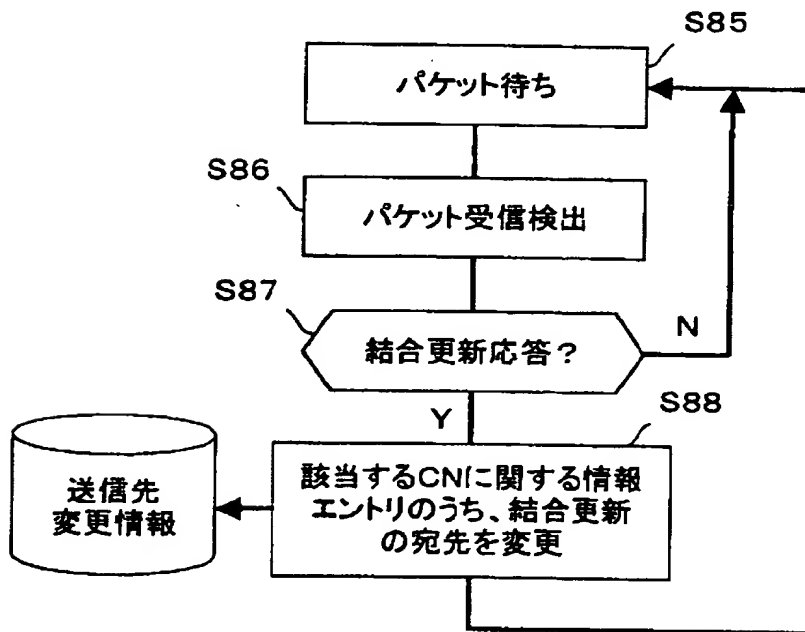
【図 1 9】

図14の実施形態におけるIPサービス制御  
メッセージ処理を示すフローチャート(その2)



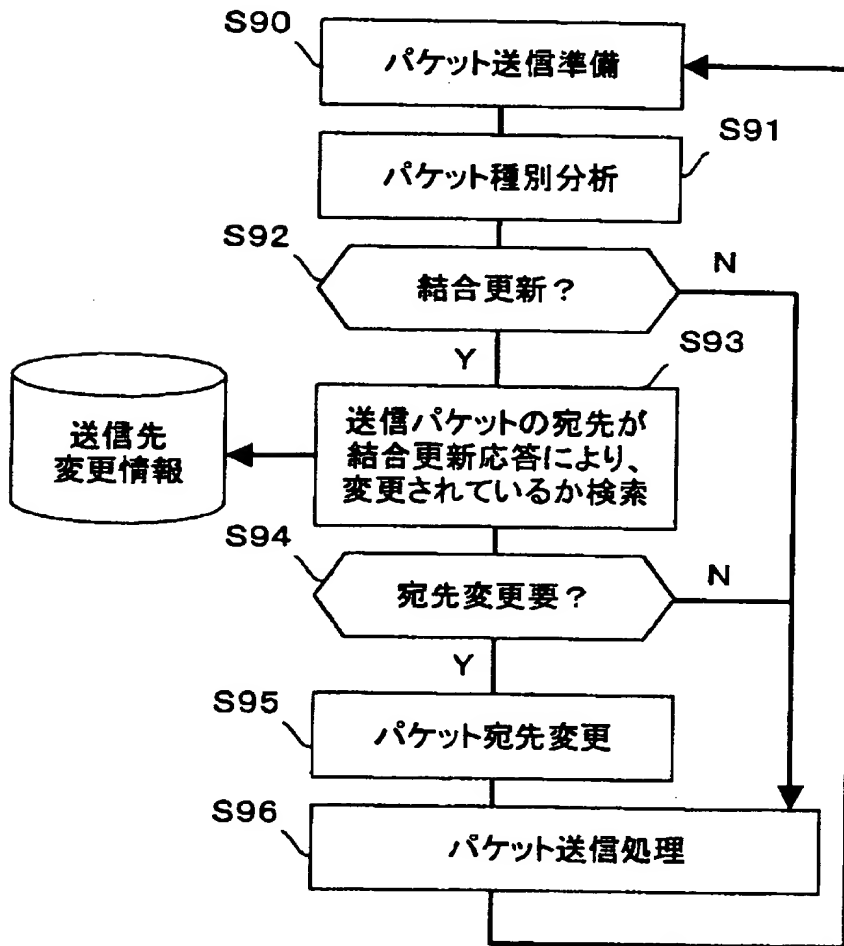
【図 2 0】

図14の実施形態におけるIPサービス制御  
メッセージ処理を示すフローチャート(その3)



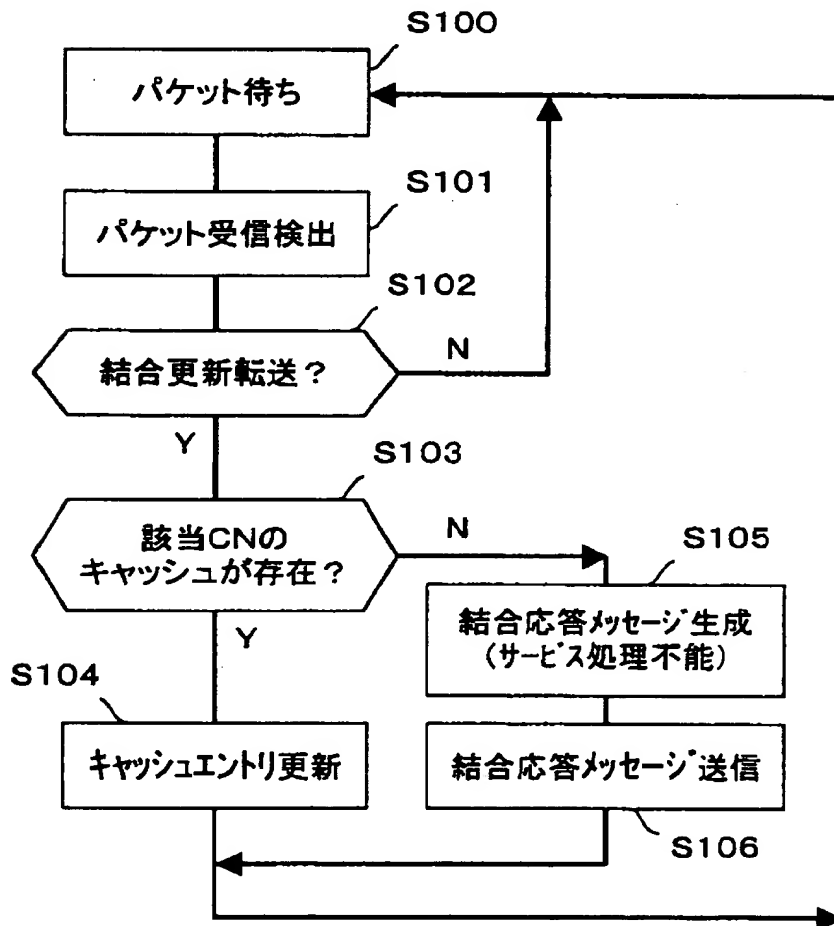
【図 21】

図14の実施形態におけるIPサービス制御  
メッセージ処理を示すフローチャート(その4)



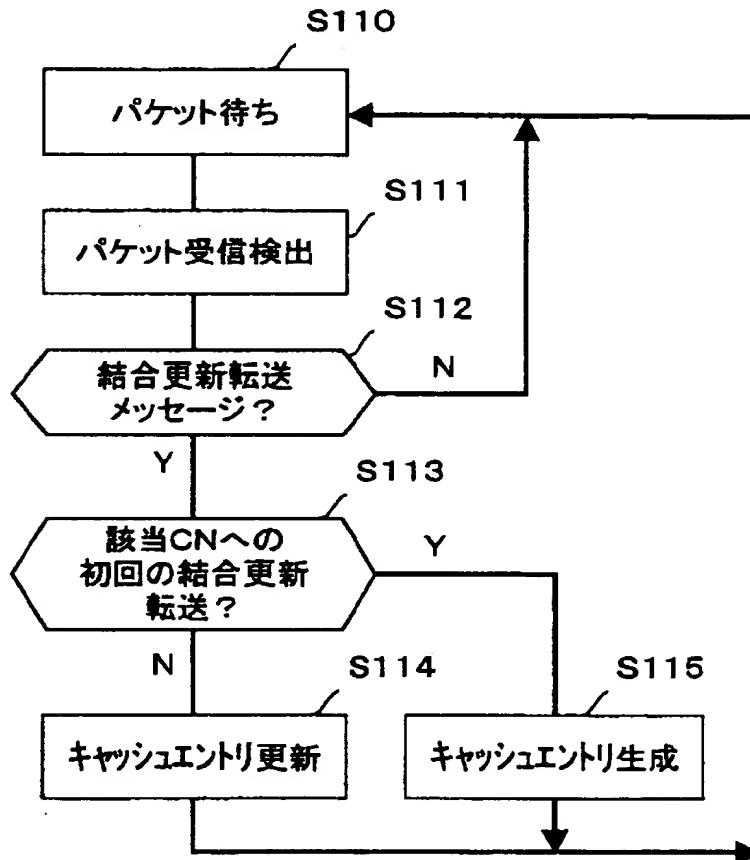
【図 2 2】

図15の実施形態におけるIPサービス制御  
メッセージ処理を示すフローチャート(その1)



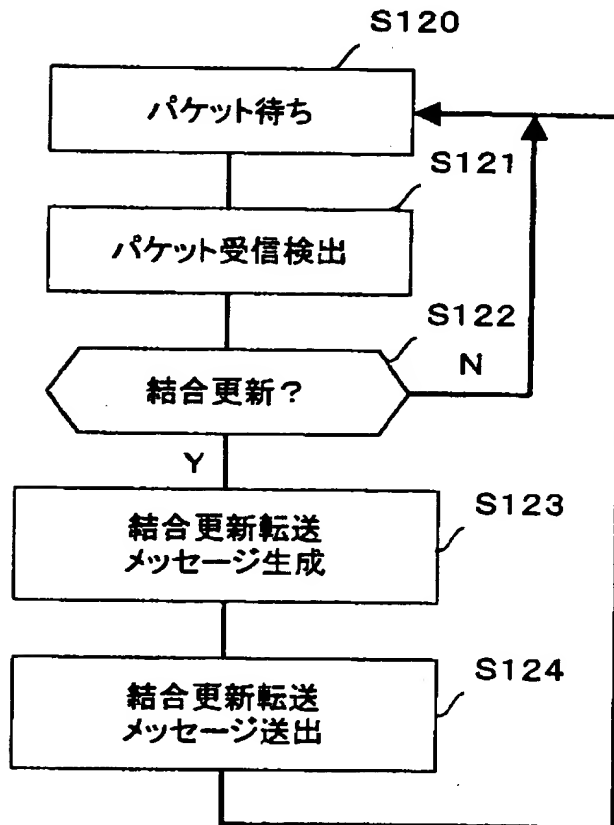
【図 2 3】

図15の実施形態におけるIPサービス制御  
メッセージ処理を示すフローチャート(その2)



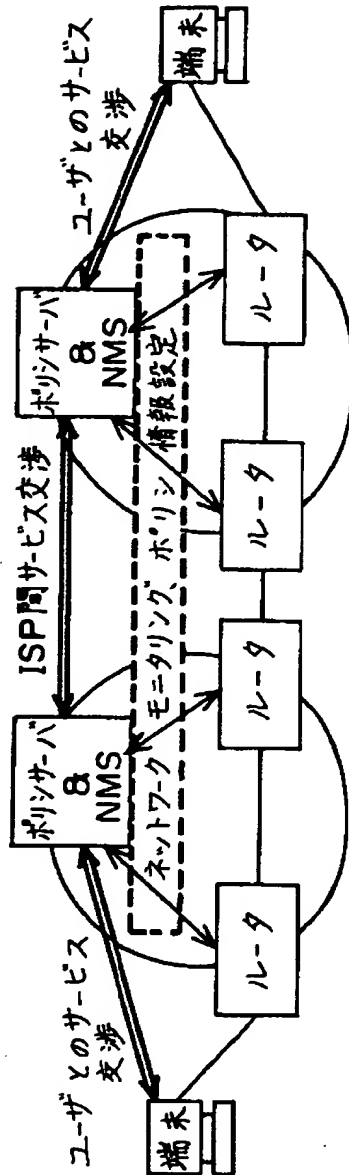
【図 2 4】

図15の実施形態におけるIPサービス制御  
メッセージ処理を示すフローチャート(その3)



【図 25】

従来技術のポリシー(Policy)による  
ネットワークにおける品質制御の例を示す図





【書類名】 要約書

【要約】

【課題】 移動端末を広範にサポートするネットワークの通信システムを提供する

【解決手段】 本来端末（CN）25と直接対応するホームエージェント26とCN25との間に、ルータであるプロキシCNを設ける。プロキシCNは、Mobile IPのサービス制御を行う。CNは、Mobile IPを使ったサービスを受ける場合、プロキシCNにアクセスし、サービスプロファイルDB27を参照するリンクレイヤ認証サーバ23によって認証を受け、ネットワークへの接続を行う。通信相手である移動端末MNとの通信は、プロキシCN24を介して行われ、トンネリングによるパケットの送信もプロキシCN24によって行われる。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社